

# Operations Analysis (Study 2.1)

## Contingency Analysis

*DRA*

Prepared by  
Advanced Mission Analysis Directorate  
Advanced Orbital Systems Division

15 July 1974

Prepared for OFFICE OF MANNED SPACE FLIGHT  
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION  
Washington, D. C.

Contract No. NASW-2575



Systems Engineering Operations  
THE AEROSPACE CORPORATION

(NASA-CR-140028) OPERATIONS ANALYSIS N74-33261  
(STUDY 2.1). CONTINGENCY ANALYSIS  
(Aerospace Corp., El Segundo, Calif.)  
65 p HC \$6.25 CSCL 22A Unclass  
63/30 17144

OPERATIONS ANALYSIS (STUDY 2.1)

Contingency Analysis

Prepared by  
Advanced Mission Analysis Directorate  
Advanced Orbital Systems Division

15 July 1974

Systems Engineering Operations  
THE AEROSPACE CORPORATION  
El Segundo, California

Prepared for  
OFFICE OF MANNED SPACE FLIGHT  
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION  
Washington, D. C.

Contract No. NASW-2575

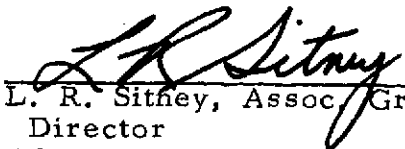
OPERATIONS ANALYSIS (STUDY 2.1)  
Contingency Analysis

Prepared by



R. R. Wolfe  
NASA Study 2.1 Director  
Advanced Mission Analysis  
Directorate

Approved



L. R. Sitney, Assoc. Group  
Director  
Advanced Mission Analysis  
Directorate  
Advanced Orbital Systems Division

## FOREWORD

NASA Study 2.1, Operations Analysis, addresses several problem areas related to future operational concepts for the Space Transportation System. Emphasis has been placed on Shuttle upper stage operations which could be employed to perform deployment, retrieval or space servicing of automated satellite programs. The October 1973 Mission Model serves as the baseline definition of the launch schedule for expendable satellite operations. This has been modified to reflect operations associated with space servicing. The Space Shuttle Payload Data Analysis (SSPDA), also issued in October 1973, was used as the baseline definition for payload design information. As a part of this study, a significant group of these payloads have been reconfigured for space servicing in which each payload is composed of space replaceable (SRU) and nonreplaceable (NRU) units.

This report forms a part of the Study 2.1 effort and addresses the potential problems that could be encountered with upper stage operations when servicing an automated satellite in geosynchronous orbit. Other reports to be issued under this study effort provide the basic space serviceable payload design data, an assessment of upper stage software complexities and cost, and the results of the space servicing logistics analysis.

Study 2.1, Operations Analysis has been performed under the direction of Mr. V. N. Huff, NASA Headquarters, Washington, D. C., Code MTE, Contract Number NASW-2575.

PRECEDING PAGE BLANK NOT FILMED

## CONTENTS

FOREWORD . . . . .	v
1. INTRODUCTION . . . . .	1-1
2. GROUND RULES AND ASSUMPTIONS . . . . .	2-1
3. STUDY APPROACH . . . . .	3-1
4. CONTINGENCY FAULT TREES . . . . .	4-1
5. RESULTS AND CONCLUSIONS . . . . .	5-1
5.1 Hardware Design . . . . .	5-1
5.2 Redundancy Levels . . . . .	5-1
5.3 Manned Interactive Support . . . . .	5-2
5.4 Payload Failure Isolation . . . . .	5-3
REFERENCES . . . . .	R-1
APPENDIX . . . . .	A-1

PRECEDING PAGE BLANK NOT FILMED

## FIGURES

2-1	Space Servicing Operations . . . . .	2-2
2-2	Space Servicing Interface Schematic . . . . .	2-4
2-3	Rendezvous and Docking Sequence . . . . .	2-6
2-4	Service Unit . . . . .	2-7
2-5	Service Unit Details . . . . .	2-9
2-6	Space Serviceable EOS . . . . .	2-10
3-1	Fault Tree Analogy. . . . .	3-2
4-1	Service Mission Fault Tree . . . . .	4-2
4-2	Tug Failures Resulting in a Catastrophic Collision. . . . .	4-4
4-3	Payload Failures Resulting in a Catastrophic Collision. . . . .	4-5
4-4	Service Unit Failures Resulting in a Catastrophic Collision . . . . .	4-7
4-5	Tug Failures Resulting in Failure to Rendezvous . . . . .	4-10
4-6	Service Unit Failures . . . . .	4-11
4-7	Payload Failures Resulting in Failure to Rendezvous . . . . .	4-12
4-8	Service Unit Fails, Precluding Servicing . . . . .	4-15
4-9	Payload Failures Which Preclude Servicing . . . . .	4-16
4-10	Tug Failures Which Preclude Servicing . . . . .	4-17
4-11	Failures Precluding Payload Separation . . . . .	4-18

## 1. INTRODUCTION

The main thrust of the effort under Operations Analysis (Study 2.1) has been directed at the investigation of automated space servicing of payloads using a Shuttle upper stage as a means to reduce future program costs. One of the concerns regarding automated space servicing has been the complexities associated with responding to contingencies. For this reason, serious consideration has been given to placing man-in-the-loop to control the upper stage during servicing operations. A completely autonomous operation has very little capability to cope with contingencies if, in fact, they could develop. However, extensive manned interfaces and control center functions inherently result in complex and costly operations. Therefore, this effort was originated to assess potential contingencies associated with space servicing and determine to what degree, if any, manned interactive support should be employed. This output is then used in Reference 1 to provide a basis for estimating upper stage software costs.

In the context employed in this effort, contingencies imply occurrence of some event which causes action to be required beyond the nominal planned operations. Contingencies may evolve from payload, upper stage, or service unit failures occurring during the servicing process. Contingencies occurring prior to or after servicing are considered to be part of the "deploy" or retrieval operation and do not impact on the servicing problem. In addition, failures at the mission control center which could precipitate a contingency in orbit during servicing are assumed to be negligible and are therefore not addressed.

Finally, in any task of this type it is necessary to use a good deal of judgment as to how contingencies should be traced. The fundamental questions are: is manned interactive support required and, if so, to what extent? Therefore, the analysis is carried only to a depth necessary to provide rational answers to these questions. The analysis may be extended to derive design criteria for redundancy or operational procedures; however, a baseline upper stage definition would be required beyond that employed for this effort. In this study it is not necessary to define subsystem equipment, but only subsystem functions.

The final design solution for the Shuttle upper stage equipments should not materially alter the results or conclusions of this effort, with one exception: it is assumed that the upper stage has sufficient performance capability to perform space servicing, otherwise the question is academic.



## 2. GROUND RULES AND ASSUMPTIONS

This analysis is limited to some extent by the lack of a firm upper stage definition. For this reason, certain ground rules and assumptions are required relative to the design and operation of the upper stage when performing space servicing. It is also necessary to make specific assumptions relative to the payload. With these in hand, it is then possible to assess contingencies which could occur during the servicing operations. The results may be altered if the design and operational concept are significantly changed but, for the most part, exact equipment definitions are not required. It is only necessary to define the functions, since these should be common, no matter what equipment definition is finally employed in the upper stage design. The only questions of interest for this study involve whether or not manned interactive support is required and, if so, to what degree? It is possible to extend the fault trees, with reliability functions to aid the hardware definition, but this is beyond the current objectives.

Servicing operations are assumed to be initiated by some failure or warning action emanating from the payload in orbit. It has been assumed that the payload user will have the responsibility for identifying the failure condition, isolating the failure to a given space replaceable unit (SRU), and notifying the mission control center that a service mission is required. The user will then support the servicing operation when it occurs by placing the payload in a serviceable configuration, that is, three-axis stabilized and oriented to receive the upper stage docking mechanism. A schematic of the operational approach is shown in Figure 2-1. In addition, all appendages must be retracted away from the docking path of approach. When configured for servicing, the payload can be powered down to a quasi-dormant condition to minimize the possibility of false signals altering the payload configuration. The payloads must have corner reflectors compatible with the upper stage laser radar system to support rendezvous and docking. These reflectors should be positioned to provide a reference for the relative roll angle between the payload and the upper stage.

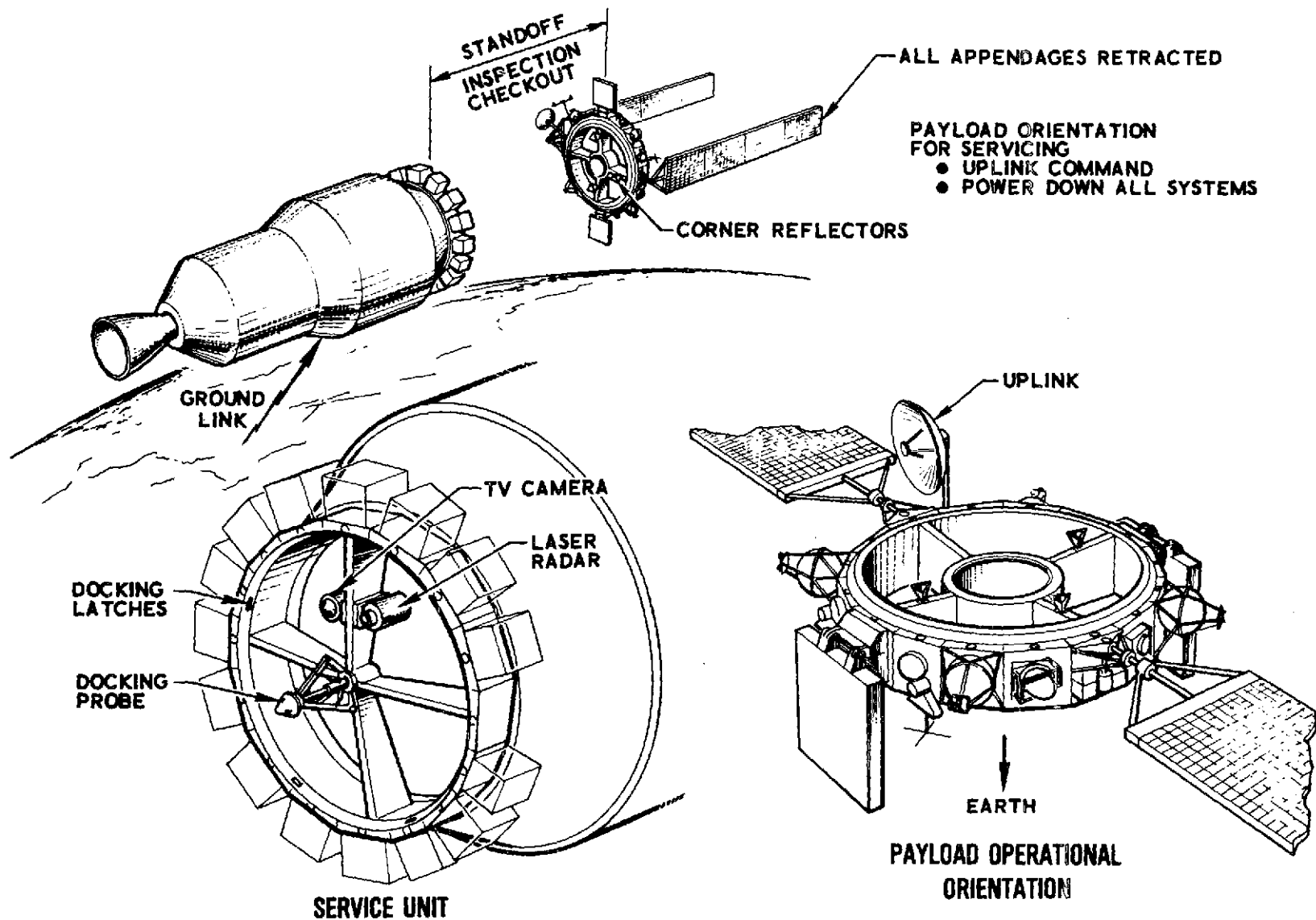


Figure 2-1. Space Servicing Operations

Once an SRU has been identified for replacement, it is loaded into a service unit along with other SRUs for the same or other payloads of the same orbital characteristics. When a sufficient load has been achieved, the upper stage (with a service unit and the SRUs) is deployed in low-earth orbit by the Shuttle. The upper stage then transfers to geosynchronous orbit in an autonomous manner, as is currently done with the Titan IIIC transtage. Under normal conditions (including ~~30~~ dispersions), the upper stage guidance system inserts the stage within laser radar range of the first payload to be serviced. A laser search mode is then initiated automatically and lock-on performed in a normal manner.

The rendezvous maneuver then progresses, based upon the laser radar signals, to the point of impact. A hard dock is performed and the service unit latched to the payload. Prior to docking, it may be desirable to perform a standoff inspection maneuver. This would employ a video camera with a display in the mission control center. All payload functions are deactivated to prevent interaction with the upper stage control system.

Once a hard dock has been achieved, operational control is assumed by the service unit sequencer. Figure 2-2 provides a schematic diagram of the interfaces between the upper stage (Tug), service unit and the payload when hard docked for servicing. The service unit is indexed to a known detent and the sequence then proceeds through removal of the identified failed SRU and replacement with a new article. The sequence would be repeated if more than one SRU is to be replaced. The service unit is essentially a self-contained unit except for the communications link. This minimizes the impact on the upper stage which is designed for a wide variety of missions. This concept was employed for the contingency analysis to follow.

Several points deserve to be addressed regarding these interface definitions. It appears prudent to minimize power transfer across any interface. Therefore, a concept has been selected with each element independent of the other, except for signal transfers across the interface.

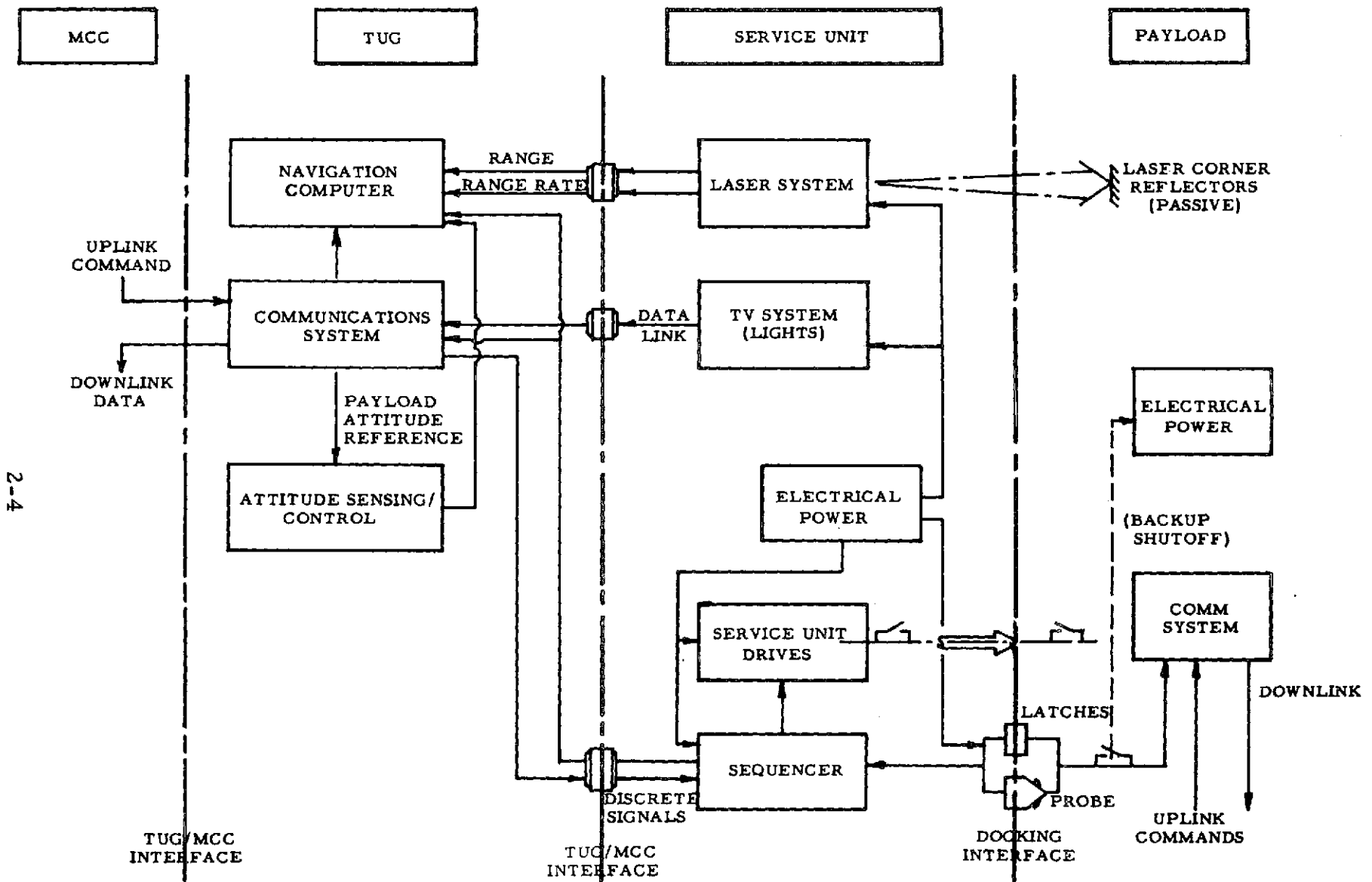


Figure 2-2. Space Servicing Interface Schematic

This is particularly true with the upper stage and the service unit interface. The laser and TV systems have been placed on the forward part of the service unit to provide adequate viewing for acquisition and docking with the payload. The sensed data is relayed to the upper stage navigation computer and the communication subsystem. If necessary, the command link can be employed to override the discrete commands generated from within the navigation computer.

Discrete commands will be received and issued by the service unit sequencer. The sequencer must receive a command or an enable to initiate the various sequences required to change out modules. After SRU transfer has been completed, the sequencer must issue a discrete to the upper stage to initiate undocking with the payload. The upper stage would then perform a standoff maneuver while the payload is checked out by the user ground operations center. If the checkout is successful, the upper stage is reinitialized and the mission is continued. If checkout is unsuccessful or marginal, the user may elect to recycle the operation or to retrieve the payload if the problem warrants. This is dependent upon the remaining performance of the upper stage. A representative timeline of events and actions is provided in Figure 2-3.

It should be noted that approximately 2.5 hours have been allocated for payload checkout after servicing. In the time period of interest, it is anticipated that automated checkout procedures will be employed. Therefore, the majority of this time is to allow repositioning of appendages and reorientation of the payload, if required. Increased time periods may be required for certain payloads. These may be easily accommodated but a detailed review would be necessary to assure that the seven-day operational period of the upper stage is not violated.

A candidate space servicing unit design is shown in Figure 2-4. This concept has been developed at The Aerospace Corporation (Ref. 2) and represents a viable, but not necessarily an optimum approach. For this study,

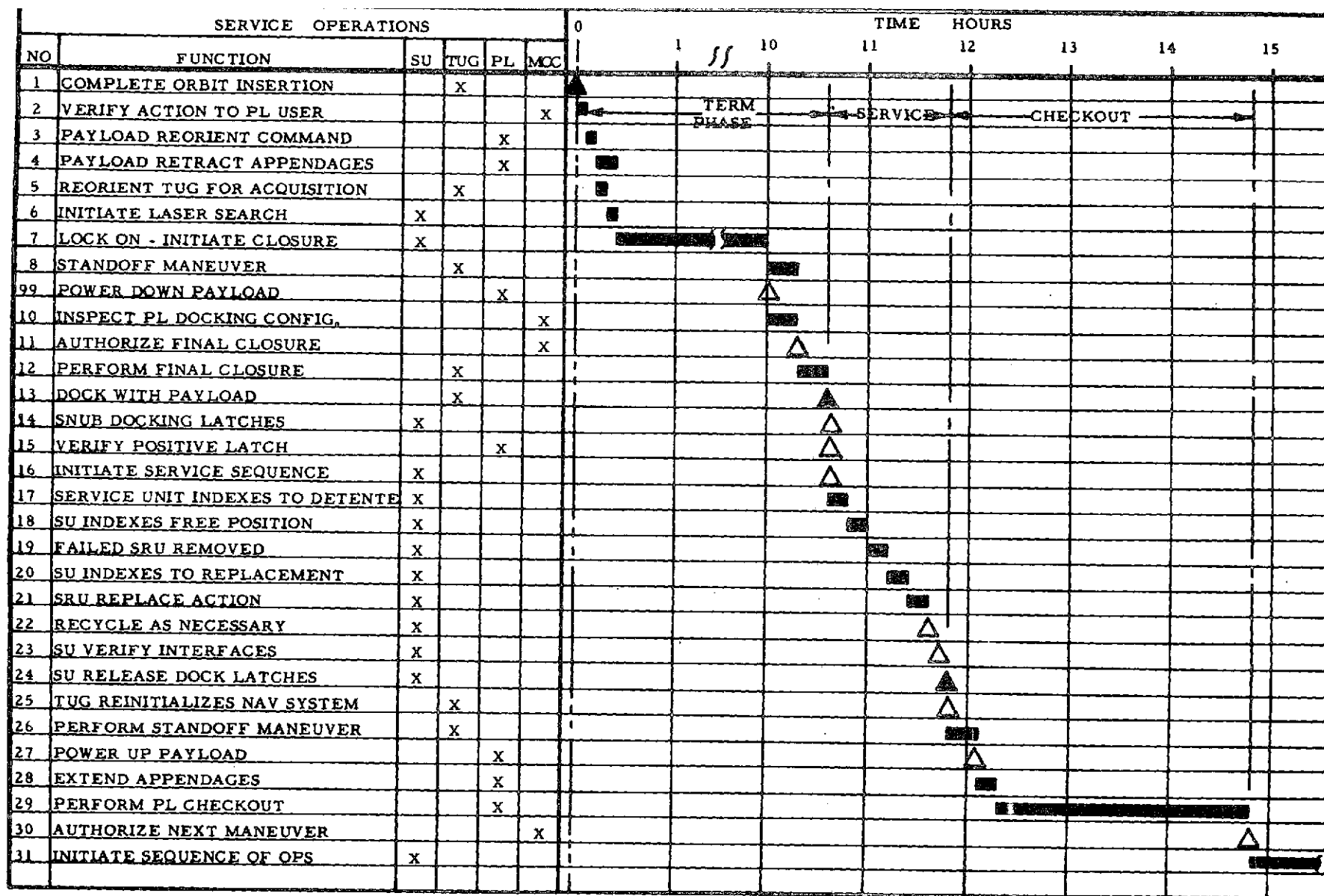


Figure 2-3. Rendezvous and Docking Sequence

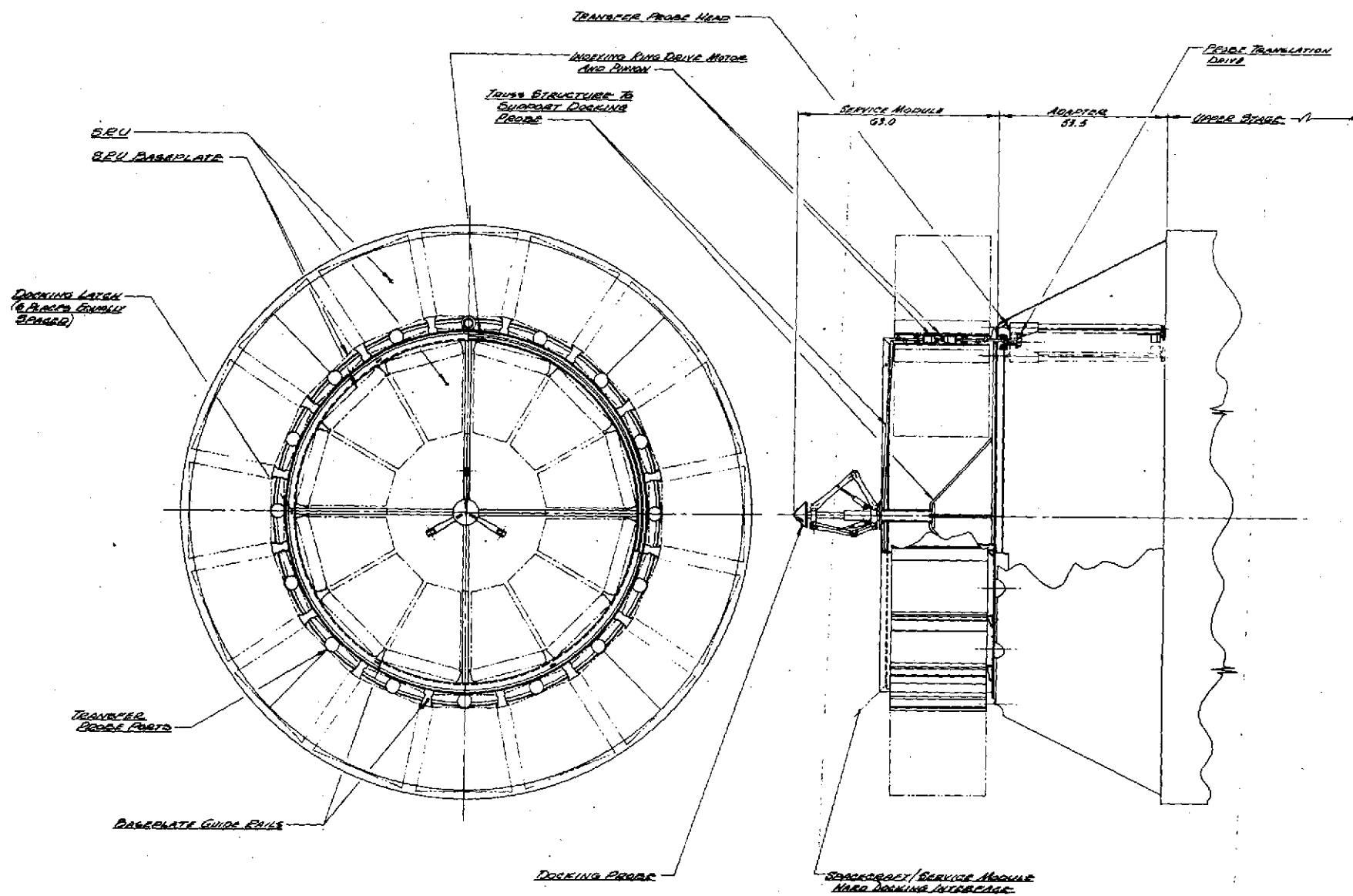


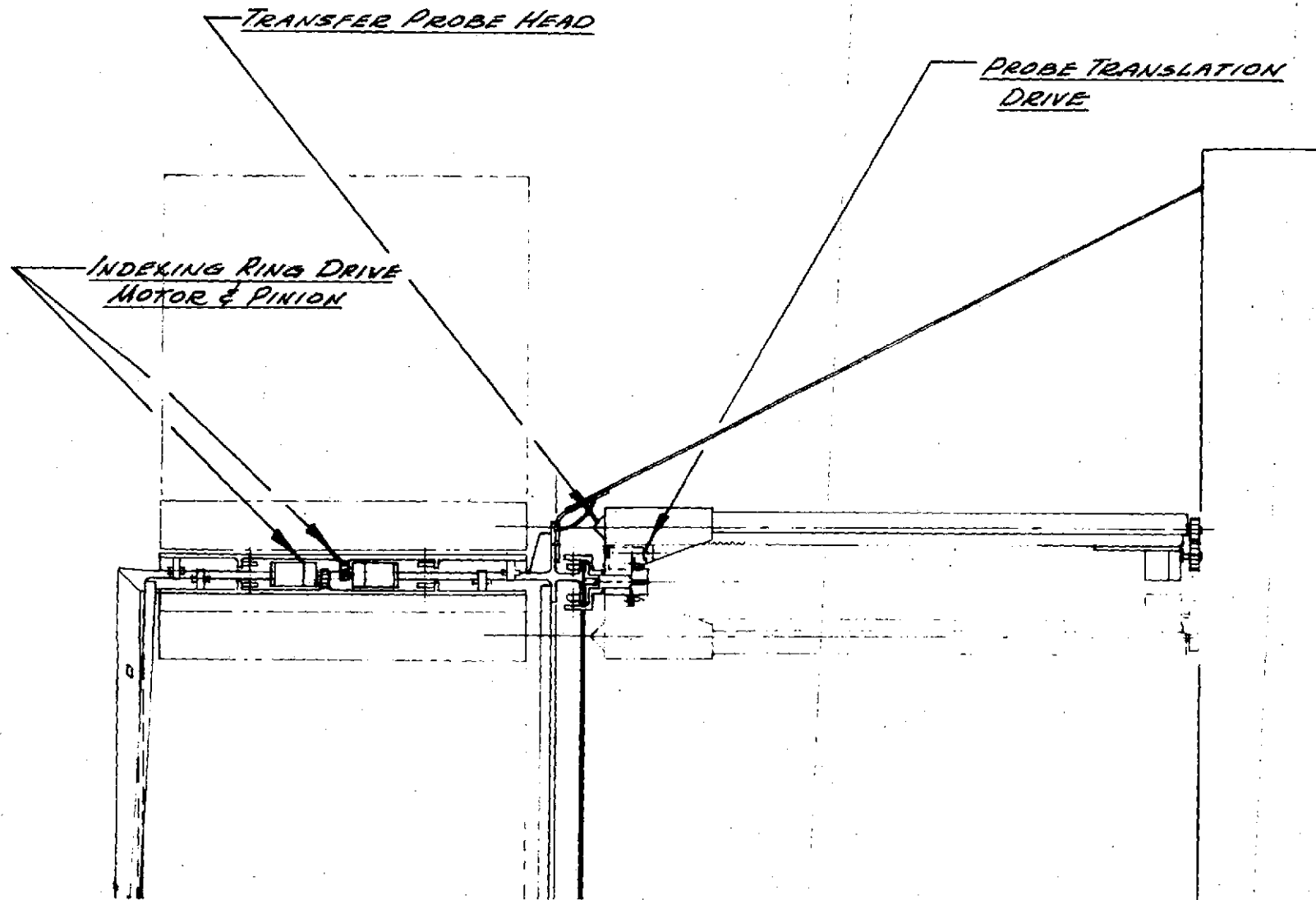
Figure 2-4. Service Unit

it is necessary only to understand the functions involved, since these will be common to most concepts under consideration. Spare SRUs are loaded onto the service unit as shown. One slot always remains empty. After a hard dock with the payload is achieved, the module to be replaced is retracted into this spare slot. The service unit ring frame is then indexed to the proper replacement position and the new SRU is inserted into the vacated slot on the payload. The design concept shown employs redundant drive motors, as demonstrated in Figure 2-5, for both the ring frame index motion and the translate plunger motion. Other approaches could be just as valid, but this is sufficient for the current effort.

In addition, it should be noted that replacement SRUs are not confined to the representative boxes shown in Figure 2-4. Elements may exceed these confines in any of three dimensions. An example is shown in Figure 2-6, indicating SRU placements for launch servicing and operational positions on a space serviceable Earth Observatory Satellite (Ref. 2). It is necessary to fold the oversized SRU during launch. Prior to servicing, the oversize element would be extended in a peripheral direction to allow an unobstructed docking face. The mechanisms for retraction or extension would be exercised by discretes issued from the service unit sequencer. After servicing, the particular SRU involved is repositioned to an operational position.

The above scenario attempts to define a concept of operation which may or may not require manned interactive support. Many if not all of the functions could be automated. Automation of the rendezvous and docking maneuver is certainly within the current state of the art. SRU exchange is a straightforward sequence of events which can be easily preprogrammed prior to liftoff. In the event several satellites are to be serviced requiring an extended time period, it may even be possible to operate the upper stage without a ground navigation update. Since the ephemeris of each satellite must be known to a high degree of accuracy, it is reasonable for the upper stage, after docking to reinitialize the navigation computer to the known satellite state vector.





2-9

Figure 2-5. Service Unit Details

Figure 2-6. Space Serviceable EOS

Consequently, if manned interactive support is required, it will be for the purpose of accommodating unknown contingencies, requiring reasoning and logic which cannot be readily preprogrammed. Although automated systems may appear complex, it should be recognized that the addition of command receivers, decoders, increased telemetry, and display provisions for manned support inherently complicates the system design even further. Therefore, manned interactive support adds another dimension to the reliability equation and this additional complexity must be justified. This is the basic problem to be addressed by the contingency analysis.

### 3. STUDY APPROACH

The approach employed involves use of a modified "Fault Tree" technique employed in safety analyses. Application of the fault tree is not as rigorous in this case, because the objective is to assess contingencies only at the system level without going into depth relative to component failures which could precipitate an event. It is not necessary to specify all modes of failures, but only those leading to the top events of the tree. Neither is it possible or necessary to incorporate statistical data in the trees developed. The answer desired is one of judgment, addressing the need for manned interactive support from a ground command station.

The analogy to a fault tree lies in the manner of tracing potential events down to the action which could cause that event to transpire. The analogy is shown in Figure 3-1. The first level is the event to be investigated. For the purpose of this study, that event is "Failure of the Service Mission." The second level of the tree addresses the question: what major events could occur to lead to a failure of the servicing mission? Level 3 addresses "why" did this event occur, and searches for the major elements which could lead to the major event occurrence. Tracking the tree structure further to the fourth level arrives at the conditions which could occur and asks "how?" It is now possible in an orderly manner to address the subelements and subconditions which are levels 5 and 6.

"Or" gates are used to express the fact that the next higher event or condition could occur from any of the subpaths below it. An "and" gate is employed when subevents are conditional; that is, one action will precipitate to the next higher event, only if another condition exists to enable this action. Therefore, passage through an "and" gate, in general, represents a much lower probability of occurrence than passage through an "or" gate. In this way the tree helps to visualize those necessary and sufficient conditions at each level to allow passage to the next higher rung of the tree.

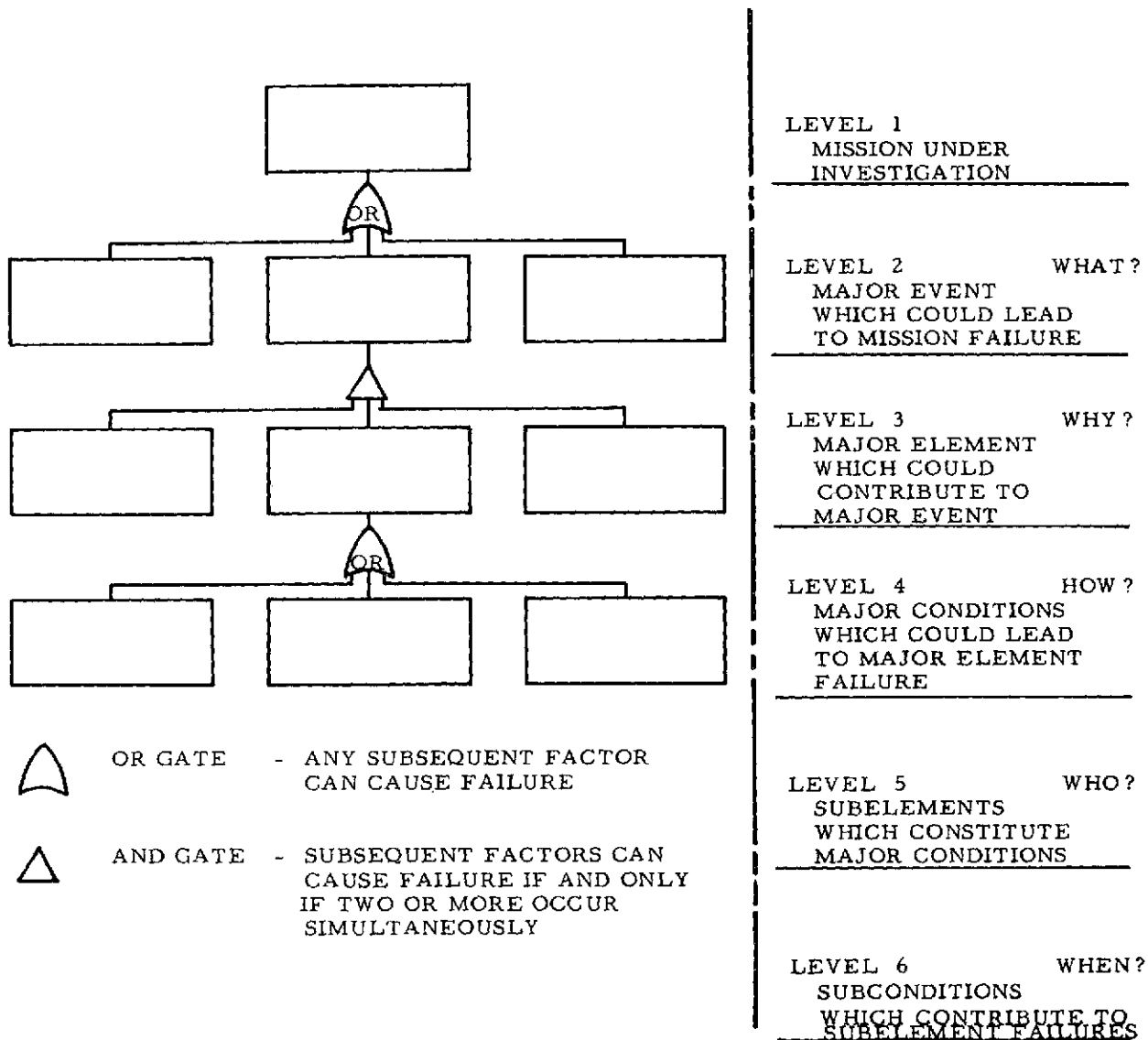


Figure 3-1. Fault Tree Analogy

Finally, it is necessary to distinguish between events and conditions because this is very important in structuring the tree. An event in the context used here represents a point in time where an action has or could occur. A condition represents a span of time over which the event could occur. The process then consists of hardware component failures at the lowest level (which are events in this sense) triggering a condition at the next level. This condition, combined with others, if necessary, pyramids to an event at the next higher level. This process continues to the top event, "Failure of the Servicing Mission." In this analysis, the tree has been structured to the conditions which exist during the servicing operation. In this way, it is seldom necessary to speculate on the type of hardware involved, but to recognize only that some hardware is required to perform the function involved.

#### 4. CONTINGENCY FAULT TREES

A total of 12 trees have been developed. The top level fault tree is defined by Figure 4-1. Lower tier trees follow as each branch is expanded. The hazard description for each numbered block of the tree is provided in table form in the Appendix. In general, each tree is carried down five levels below the top event to arrive at various subsystem functions. The tree may be expanded at any level, but the organization is such that the major events and conditions have been described and further expansion is not warranted.

The top event, Failure of the Service Mission, may be caused by any of four major events. Each one of the four events can be precipitated by failures of any one of the three major elements of the system. The major events to be considered are:

- a. Either the upper stage, service unit, or the payload fail in a manner which allows a catastrophic collision to occur (1.1).
- b. One of the three major elements fails in such a manner that, although a catastrophic collision is avoided, it is not possible to perform the rendezvous and docking maneuvers (1.2).
- c. Rendezvous and docking have occurred, but for one reason or another, the servicing functions cannot be completed (1.3).
- d. Servicing has been completed, but for one reason or another, the upper stage and service unit cannot undock or detach from the payload.

The failure to successfully complete the servicing mission does not necessarily imply loss of the payload, service unit, or upper stage. However, the emphasis here is, could manned interaction prevent loss of the mission and the attendant cost associated with a subsequent repeat performance. Altering the top event to address a specific vehicle or equipment loss would obviously force a restructuring of the fault trees.

If the upper stage failed to rendezvous, it is possible that the stage could return to the Shuttle and servicing be performed on a subsequent flight. The same could be true if servicing failed. If the payload could not be

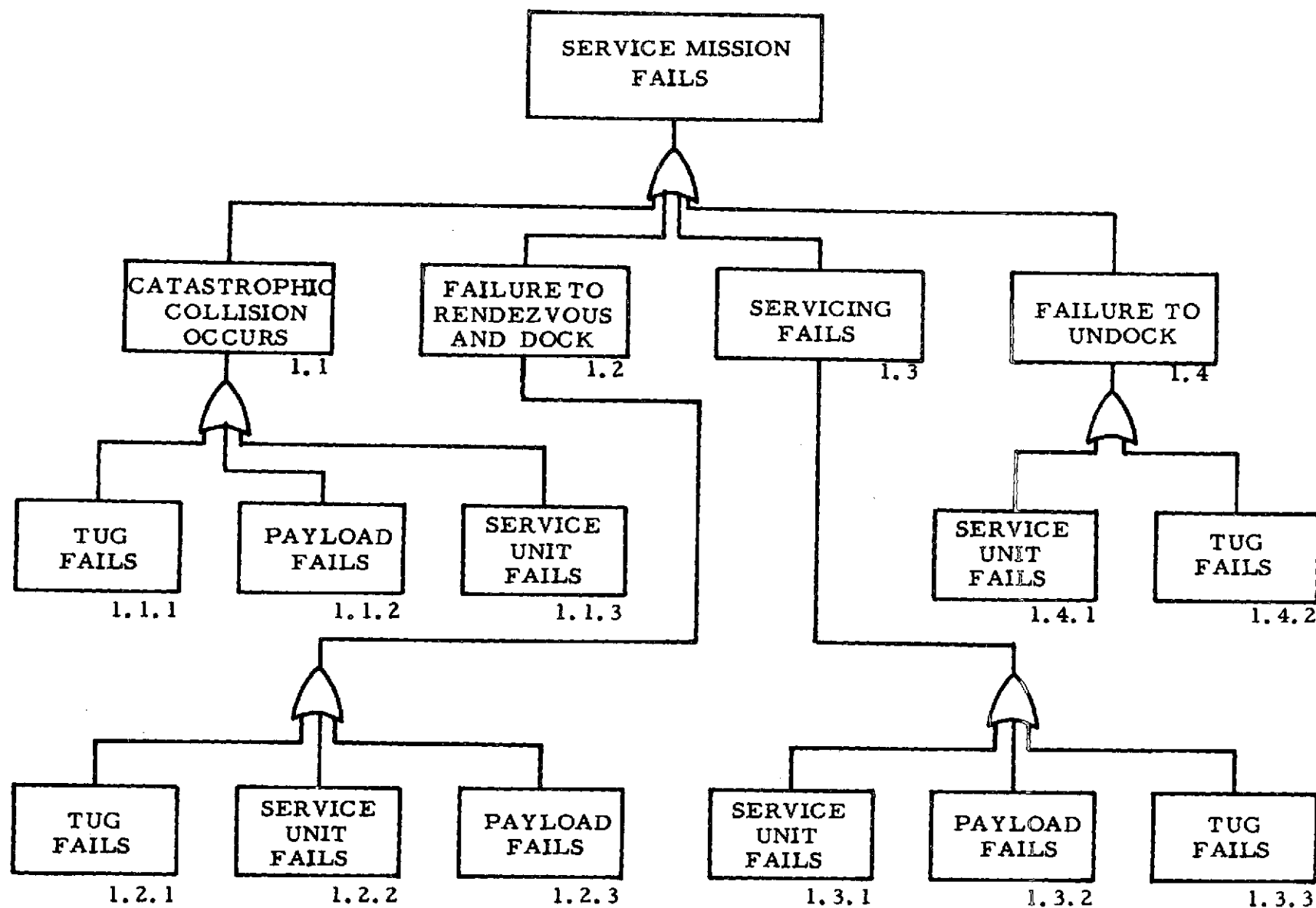


Figure 4-1. Service Mission Fault Tree



detached (failure to undock), it may be possible to bring the payload to the Shuttle in low-earth orbit, depending upon the performance capability of the upper stage. However, if a catastrophic collision occurs, it is assumed that both the payload and the upper stage are lost.

Figure 4-2 traces Block 1.1, Catastrophic Collision, through upper stage (Tug) failures. Failures leading to a collision could result from upper stage subsystem failures or failures of the steering signals to be received by the Navigation computer. Tracking Block 1.1.1.1 shows that subsystem failures only pose a threat if the upper stage and payload are on a collision course after the insertion maneuver has been performed. Normal procedure would cause the upper stage to insert below and aft of the payload. A severe overshoot would be required, therefore, to assume a collision course. Although this should be very remote, there is an additional inherent safety margin derived from the laser radar. If the upper stage subsystems are operative, the stage will perform a standoff maneuver, thereby preventing a collision. Further backup could be provided via the command link to null the relative velocity.

Consequently, it appears that adequate safeguards can be achieved with current design techniques. The command override capability will inherently exist to support retrieval of the stage by the Shuttle. Hence, this presents no problems unique to servicing. Although manned backup of a functions might be desirable, it is difficult to see where they would be required because a reasonable degree of reliability already exists with the current state of the art.

Failure of the interface signals may present different problems but the response would be similar. If the signals are lost for a period of time, the normal procedure would call for a standoff maneuver. This could easily be performed automatically and a catastrophic collision avoided.

The same is not true for payload originated failures as shown in Figure 4-3. Here it should be remembered that each payload, although space serviceable, has unique characteristics. Automatic responses to

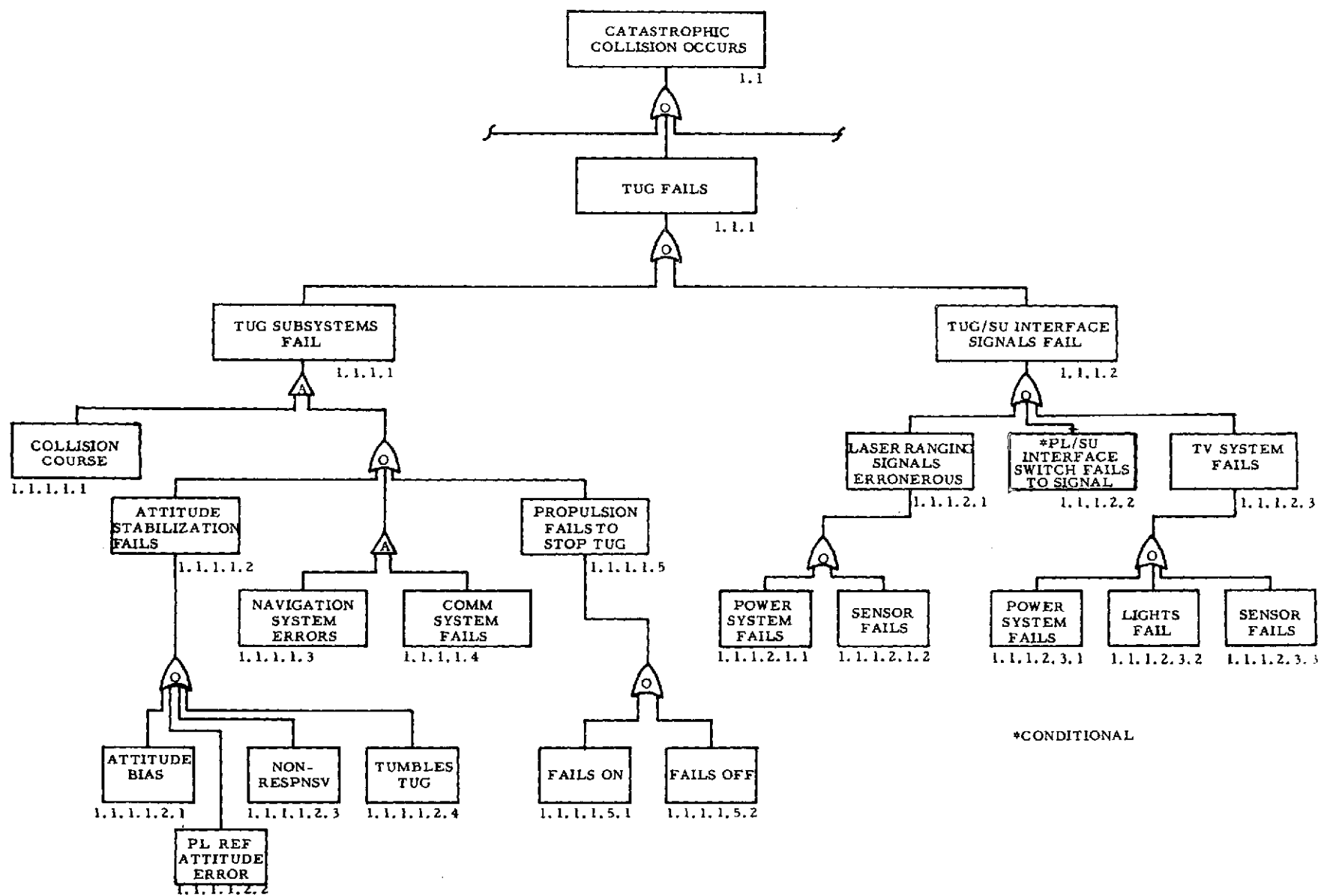


Figure 4-2. Tug Failures Resulting in a Catastrophic Collision

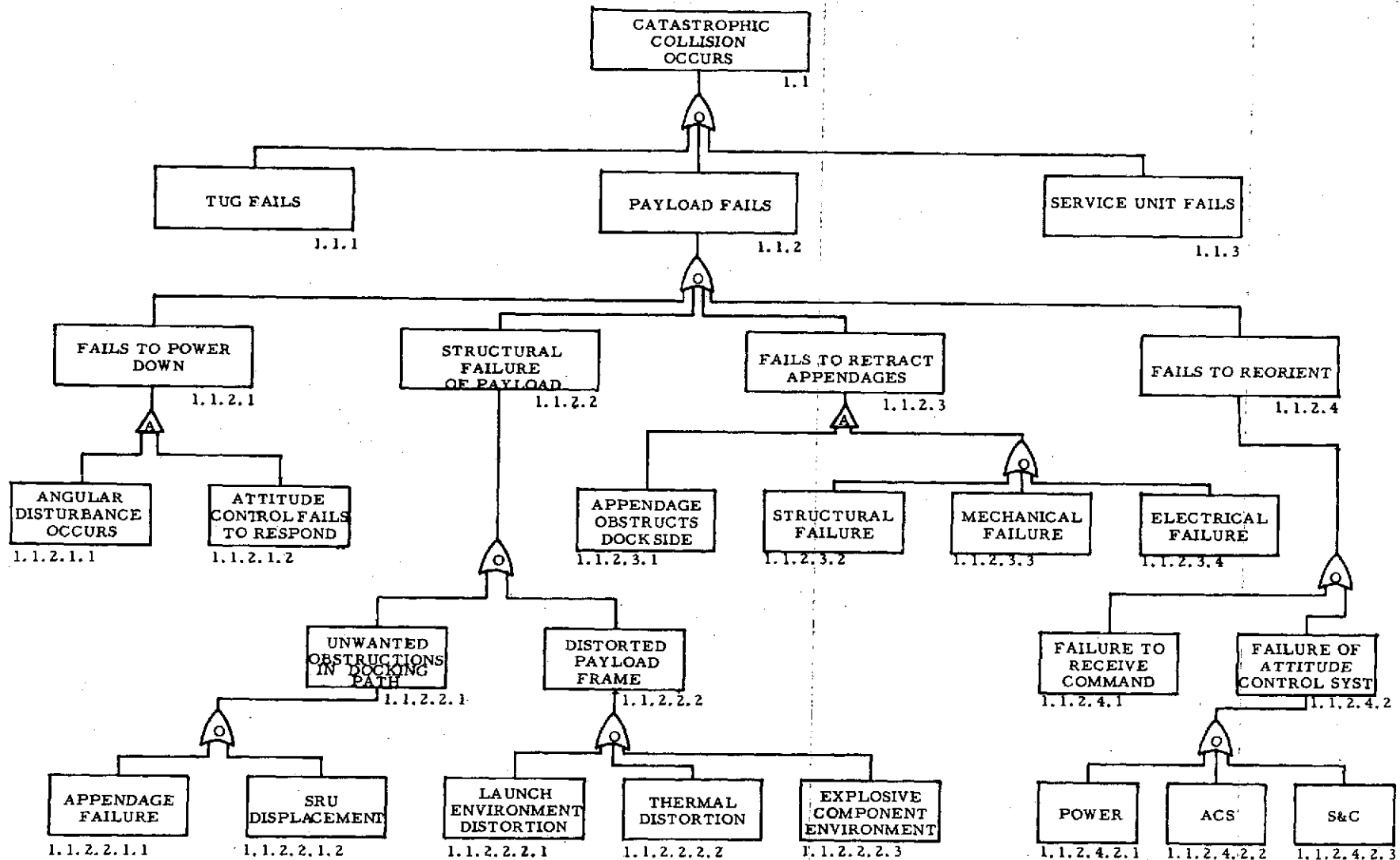


Figure 4-3. Payload Failures Resulting in a Catastrophic Collision

contingencies may not be practical. Also, experience has shown that it is not always possible to accurately predict the extent of a failure from telemetry, even though the failure could be isolated to a given SRU. A fundamental structural failure could pose a serious problem. Failure to fully retract appendages could also be serious although judicious placement out of the docking path could minimize this hazard. Therefore, mechanical and structural failures appear to provide a rational reason for concern, relative to manned interactive support.

Another branch of this tree (Fig. 4-3) addresses the question of failure to reorient for docking (1.1.2.4). This may not be required in all cases and therefore is conditional. However, it is seen that several failures could precipitate this condition. A prudent design approach with even a low level of redundancy should be adequate to preclude this condition from becoming a serious problem. Standard telemetry data is sufficient to indicate the attitude position and this information could be relayed to the upper stage operations center to postpone docking. Consequently, although this is a possible failure branch, it does not appear to demand a heavy interactive support role.

There is one more branch required to complete the catastrophic collision tree. This addresses problems that could evolve from failures of the service unit (Fig. 4-4). There is always the possibility of sensor failures, although video coverage could provide a backup to the laser to prevent a collision if man were active in the control loop. The power supply is the one element that could result in loss of both signals. Further expansion of the tree at this point would also show that a collision could occur as a result of erroneous signals. Redundant sensors could be employed but there may be a "voting" problem; hence, the alternate backup (at least to prevent a collision) of a video camera seems rational.

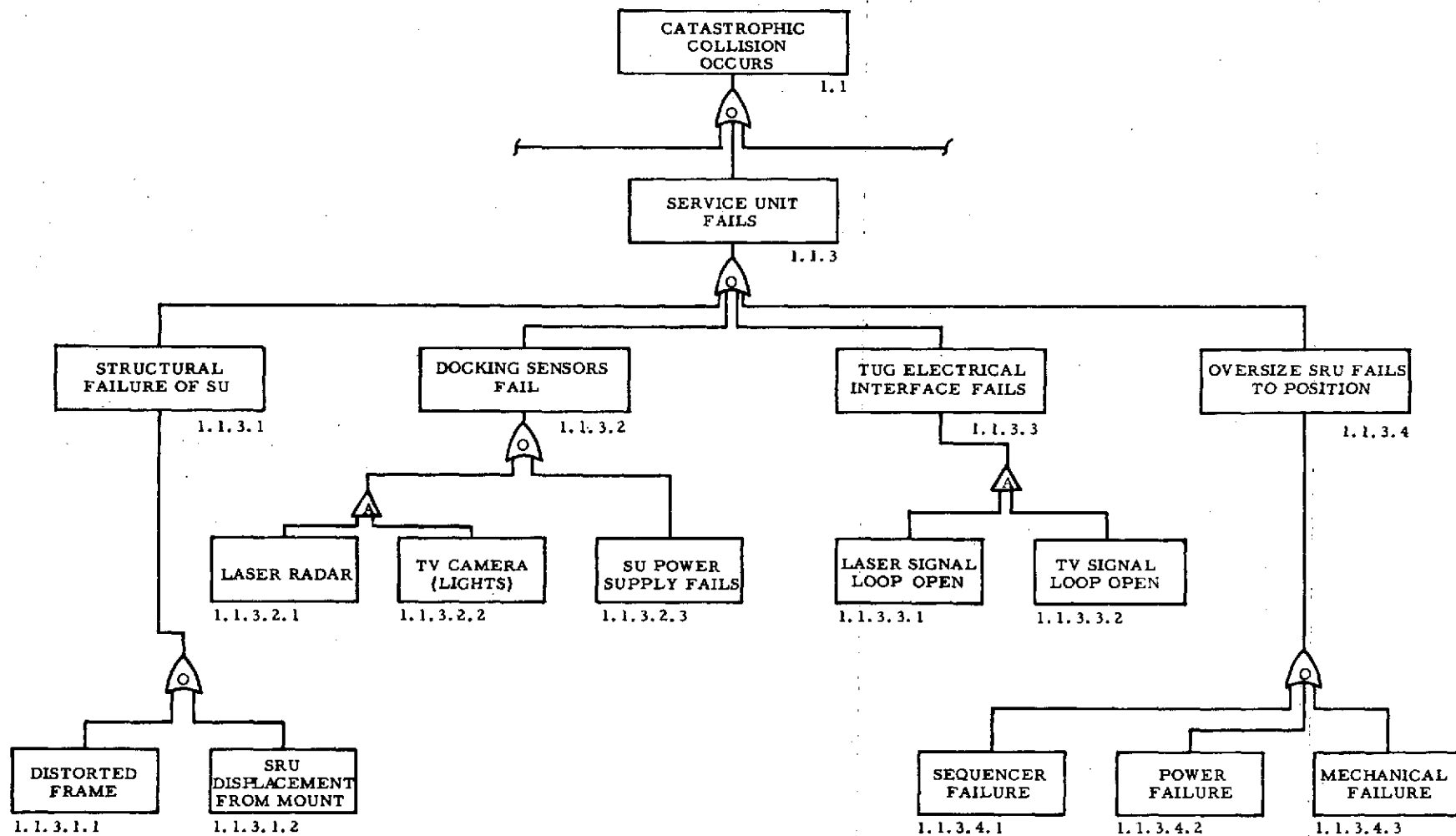


Figure 4-4. Service Unit Failures Resulting in a Catastrophic Collision

A similar condition exists if the electrical interface connectors fail, which is not at all uncommon. However, if the laser and television outputs were transmitted through separate connectors, or redundant pairs employed, this should be a minor problem. In addition, an automatic standoff could be implemented for loss of signal conditions. Therefore, these two branches do not show a need for man's intelligence in the primary loop, although as a backup it may be possible to reduce component redundancy while maintaining a rational degree of reliability.

There are two unique features that should be considered before leaving this particular branch (1.1.3). Although low in probability, it is possible that a structural problem occurs due to ascent loads, unusual vibrations, aging, or other factors. This does not require a structural failure, but merely a distortion such that the docking probe or other structural parts impact the payload improperly causing damage to the payload, service unit, or upper stage. A launch lock failure, which attaches the service unit to the upper stage, would be one example of an event that could precipitate this condition. Under these circumstances, it is difficult to visualize how manned interactive support could improve this picture. Information would have to be supplied via telemetry and the only decision to be made if a condition arises is "go" or "no-go." The thought process is dependent upon a limit switch signal or strain gauge signal which can easily be redundant and the "no-go" action automatically programmed. This may result in an occasional extra flight due to false signals but loss of the payload, Tug, or service unit would be avoided.

A similar set of conditions exists for oversize SRUs (1.1.3.4) that extend beyond the forward interface of the service unit. Prior to docking, these SRUs must be retracted away from the path of approach. Failure to do so obviously presents an obstruction which could be fatal.

Monitoring of the positioning sequence would normally be done by telemetry and again, "go/no-go" decisions could be made automatically. It might be possible to install some means of visual observation by use of fibre optics or some other device, but it is not obvious that a clear field of view would always be available. Also, since these mechanisms must have electrical connectors with the baseplate and the baseplate must receive power or signals from the service unit, there are several paths that could lead to this condition. Therefore, if visibility can be provided, manned interactive support is definitely desirable but any improvement would be constrained by the field of view.

In summary, for Event 1.1, Catastrophic Collision, the vast majority of failure conditions could be monitored and controlled automatically and the active participation of man is not required. However, there are a few unique situations indicated where, if man's intelligence could be employed it might be possible to avoid loss of a vehicle and/or loss of a payload; but the remaining trees deserve attention before taking a firm position.

Figures 4-5, 4-6, and 4-7 address the next major event leading to failure of the servicing mission. This is failure to rendezvous and dock, Block 1.2. In this series of events and conditions, the possible loss of a vehicle or payload is not a point of consideration. The loss, if it occurs, is a cost impact only and therefore the question of active manned support must be considered in a different light than in the previous conditional block. It is recognized that some of the failures that could prevent rendezvous and docking could also prevent recovery of the upper stage, but these are not peculiar to servicing and hence are not considered here. If manned interactive support were justified for other reasons, the point becomes academic for servicing. This position appears remote, however, because current operations are being performed satisfactorily without the additional complication of man-in-the-loop. It can be expected that this trend will continue unless some unique function such as space servicing breaks this barrier and requires a new approach.

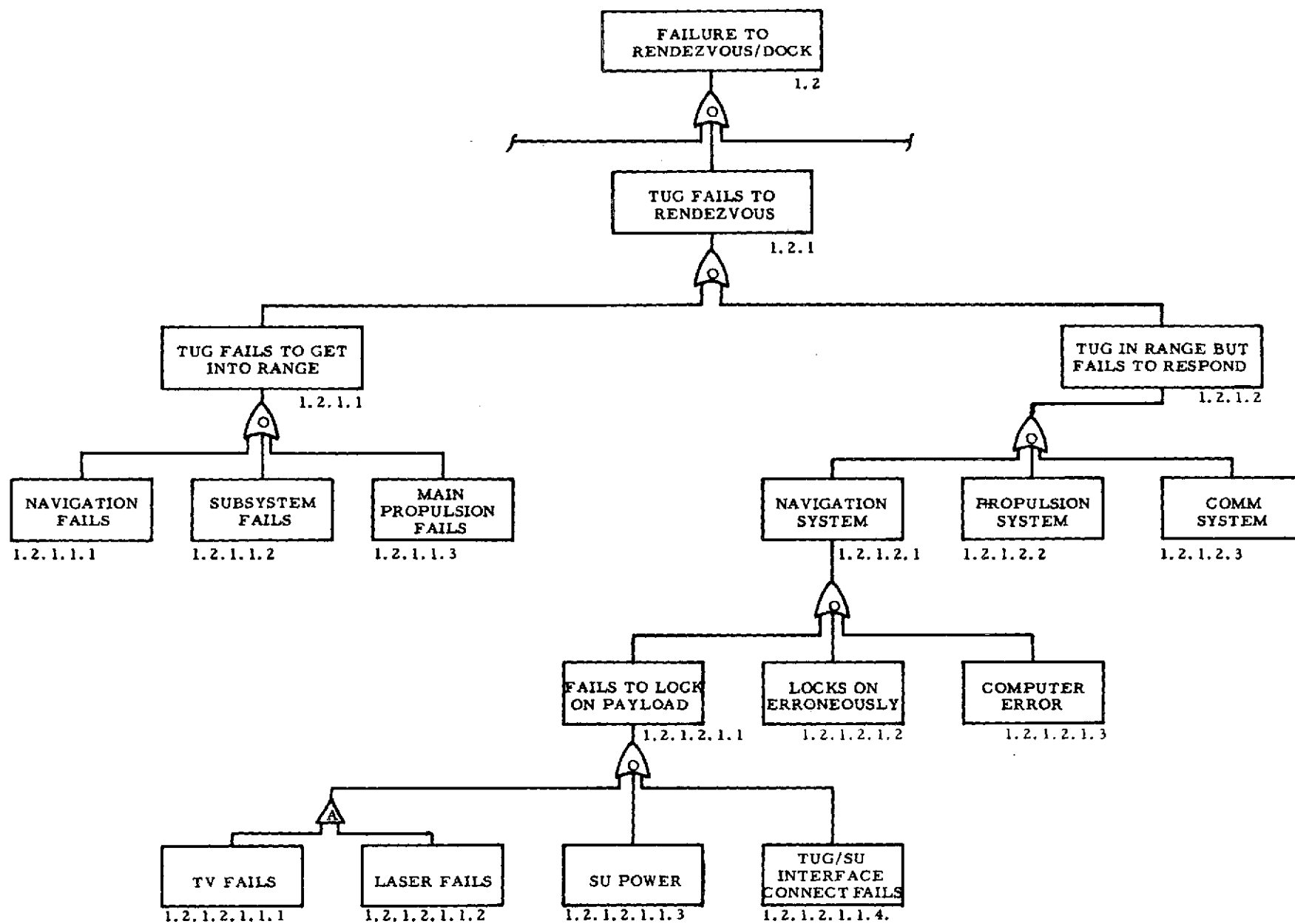


Figure 4-5. Tug Failures Resulting in Failure to Rendezvous



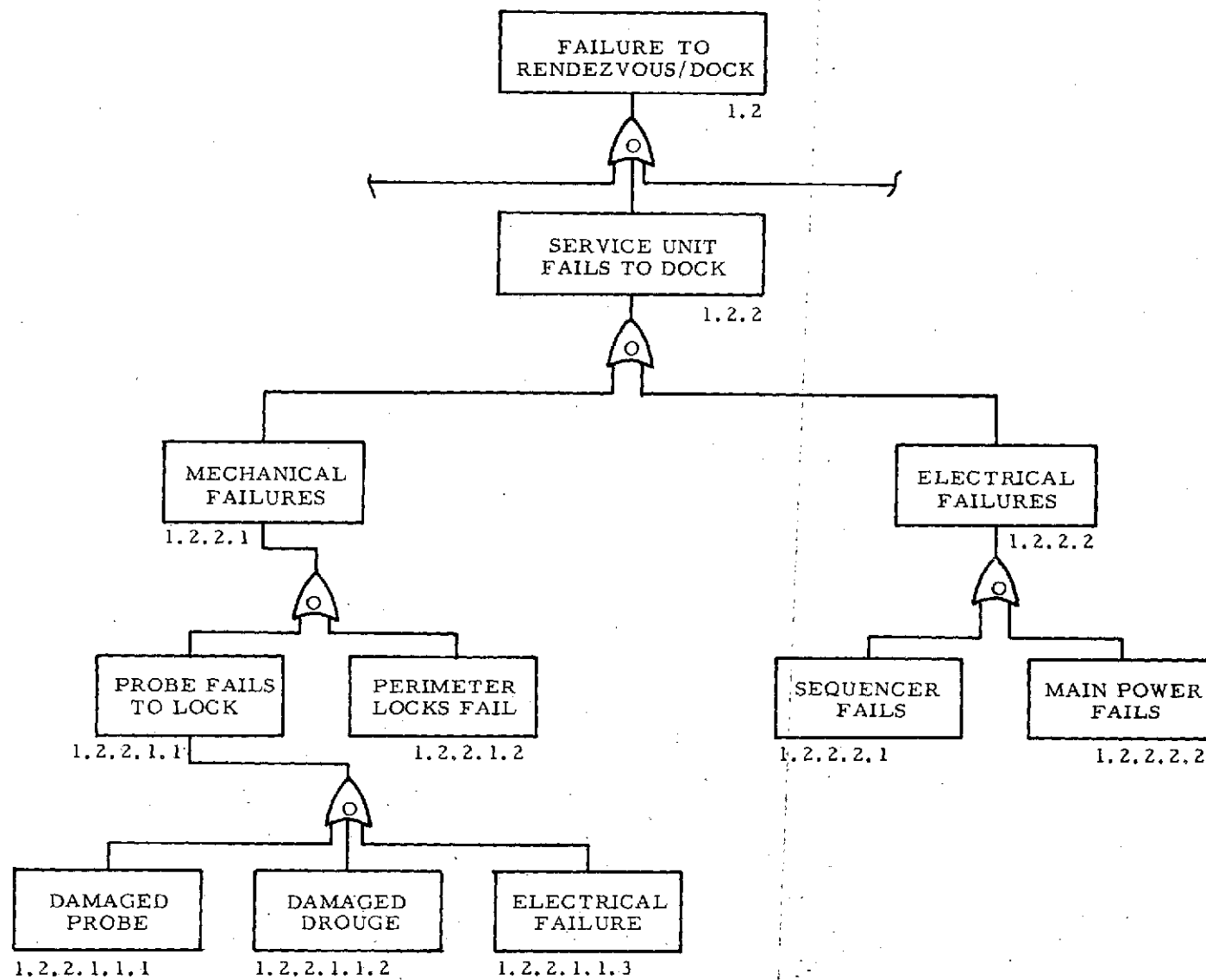


Figure 4-6. Service Unit Failures

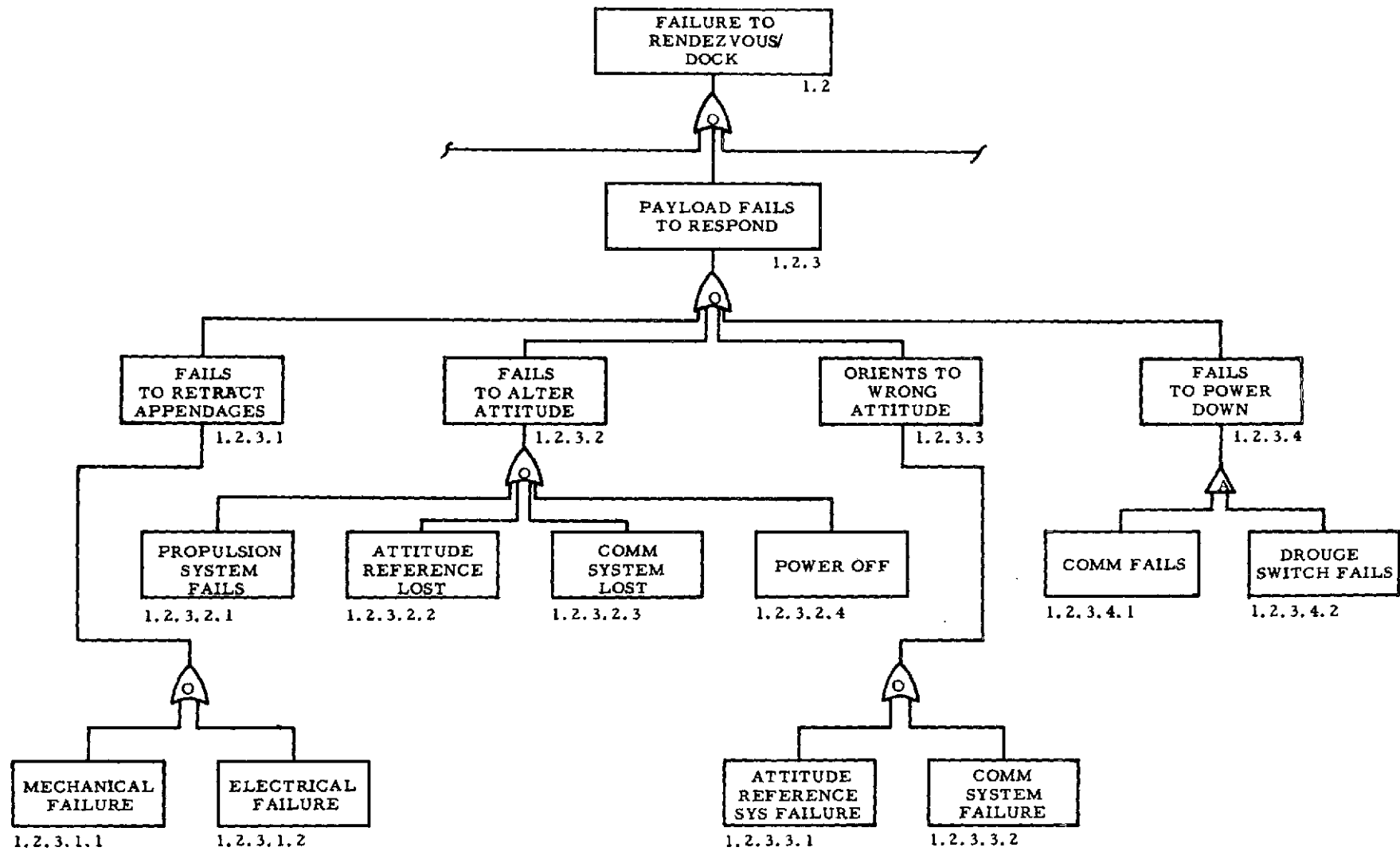


Figure 4-7. Payload Failures Resulting in Failure to Rendezvous

Block 1.2.1, Tug Fails to Rendezvous, is structured around Tug or upper stage subsystems and equipments. There are no unique requirements identifiable; however, this tree could help in the selection of redundancy criteria to assure that rendezvous is successful. Block 1.2.2, Service Unit Fails to Dock, is also relatively simple. Electrical failures are straightforward and simple redundancy can be employed to achieve a desired level of reliability. Mechanical failures are a little more difficult. The docking mechanism (in this case a probe) could fail to dock properly for any one of several reasons. It would be necessary to have a detailed design in hand to progress any further; but in general, it is assumed that at the time of engagement an electrical drive mechanism performs the snubbing action, 1.2.2.1.1.3. Pneumatic or hydraulic drives could also be employed with their own unique failure characteristics but the tree would be unaffected. The point is that there is a branch from which the failure path could develop and it should be recognized.

If these failures occur, it might be possible to recycle and try again. This could easily be automatic or be initiated by a ground command based upon telemetry data. As mentioned before, if the field of view is sufficient, it might be possible to examine the docking device by TV and determine if successive attempts should be continued. This approach is deemed to be highly impractical because the docking mechanism may be at the periphery of the service unit, similar to the perimeter locks, requiring a broad field of view. It may be possible, again with fibre optics or some other device, to perform an inspection, but at this point it does not appear very practical. The systems will have to be reliable, with adequate safeguards and automated backout procedures whether or not man is involved.

Active manned support does appear desirable for Block 1.2.3, Payload Fails to Respond. The original failure of the payload that precipitated the servicing mission could impair a proper response to ground commands

in preparation for docking. Adequate redundancy can be provided in the payload to minimize the failure to reposition the payload (1.2.3.2). However, if the failure did occur, adequate warning should be available via telemetry to indicate the payload did not respond to the repositioning command and therefore the hazard would be minimized. Reorientation to a false attitude presents a different problem. Several failures could lead to an erroneous position while at the same time indicating via telemetry that a proper attitude had been achieved. The same could be true for Block 1.2.3.1, Failure to Retract Appendages. There are obvious failure conditions which could indicate a "go" condition when in fact, docking should be avoided. The wide variety of payloads to be serviced complicates this point further, in that there may be no standard response. This inconsistency could easily lead to incorrect interpretation if telemetry data is the only source of intelligence. Active manned support appears therefore to be very desirable.

The failure of servicing operations per se are addressed in Figures 4-8, 4-9 and 4-10. There are several failure modes of the service unit that could lead to a hang-up of some kind. In general, there is no requirement for visual support but a command override capability is definitely needed. In most conditions, the action would be merely to recycle all events or switch to a redundant element. A large part could be easily automated but potential obstructions in gearways and guideways could require reordering of what might have been an automated sequence. Manned support is therefore desirable, but visual contact is questionable.

The final tree of this study addresses the inability to undock from a payload after servicing has been performed, Figure 4-11. The payload is essentially dormant, otherwise, docking could not have been performed initially. Consequently, the payload does not enter into this fault tree. There are failures which could definitely require unique sequences of operations for the service unit to extricate itself from the payload.

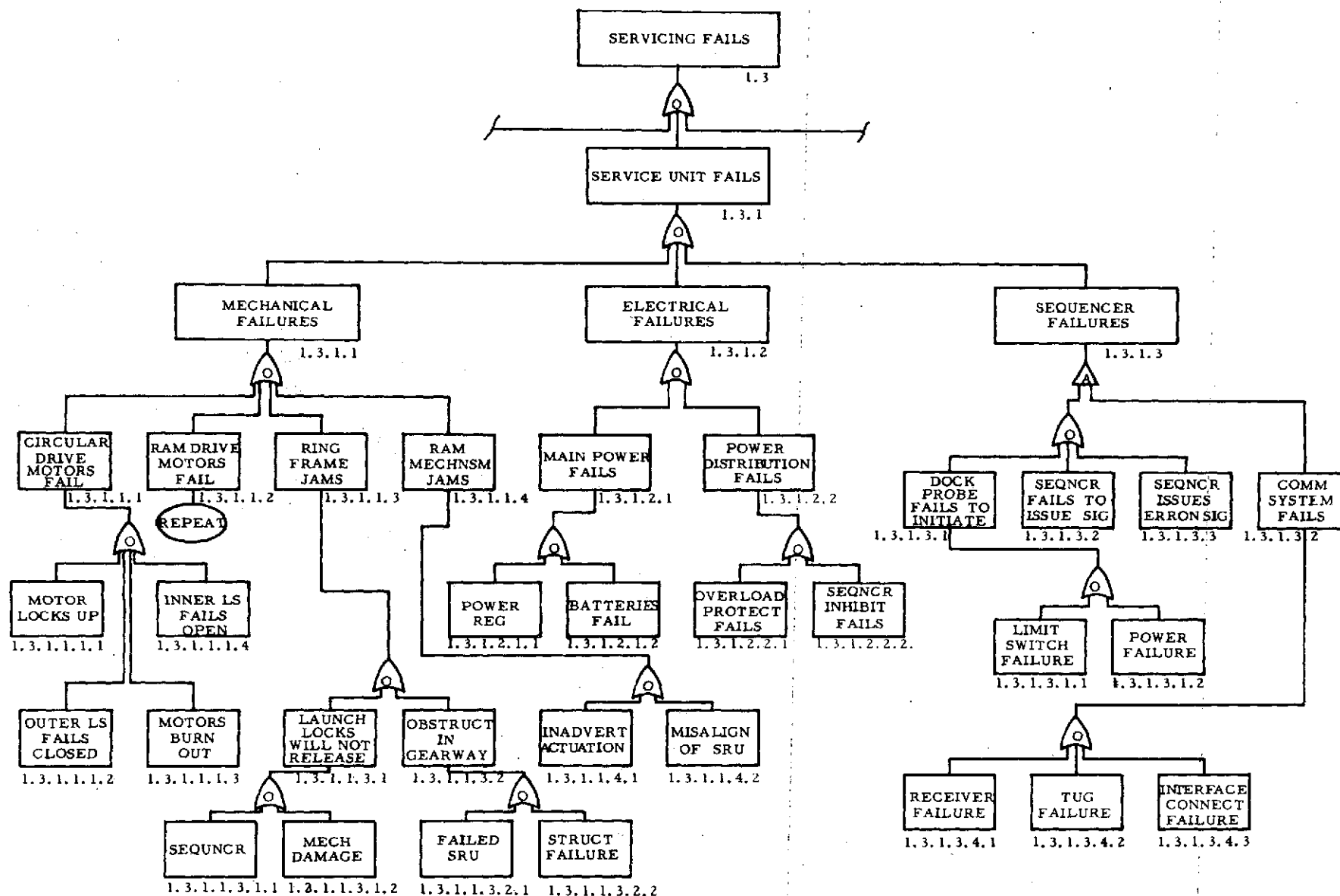


Figure 4-8. Service Unit Fails, Precluding Servicing

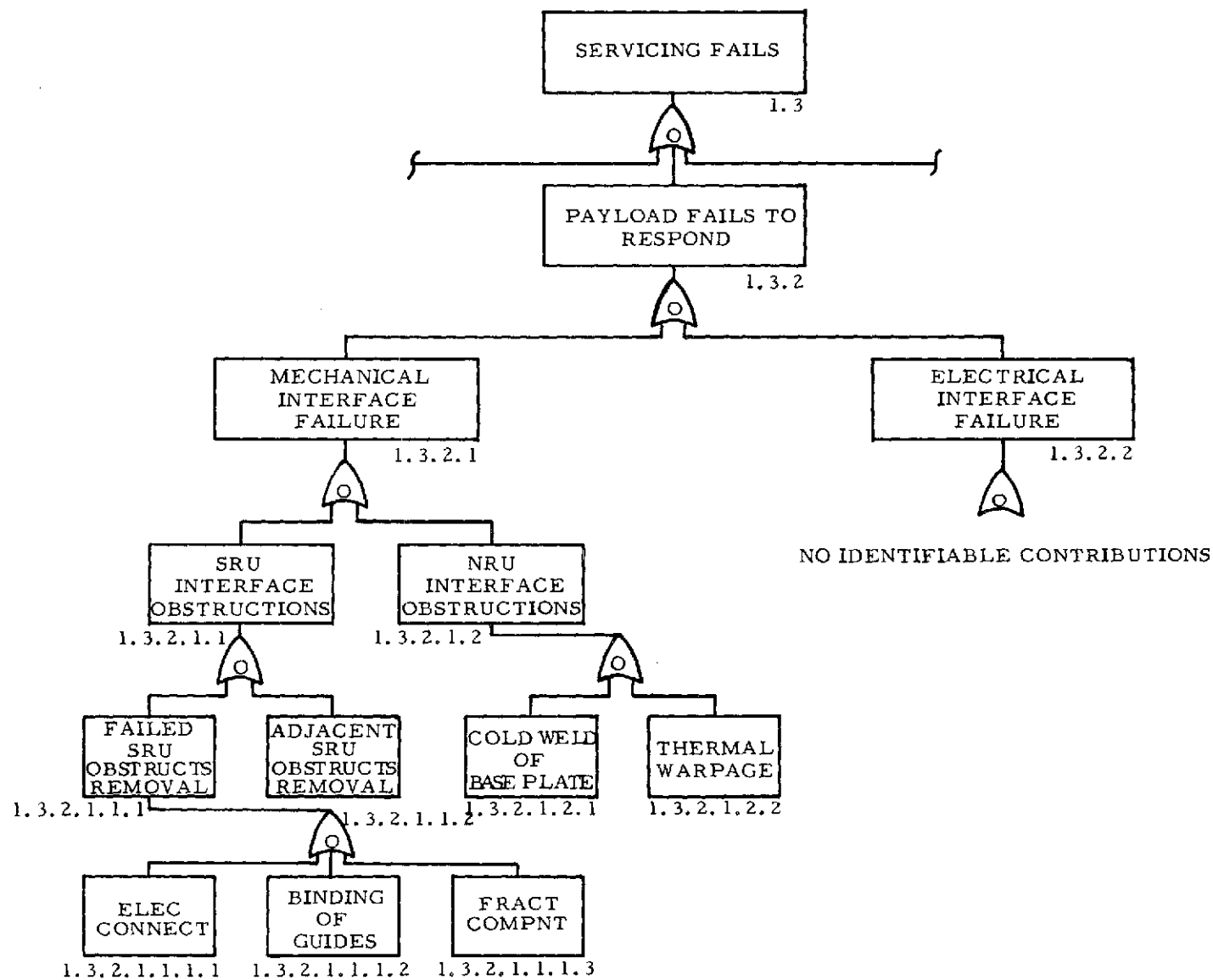


Figure 4-9. Payload Failures Which Preclude Servicing

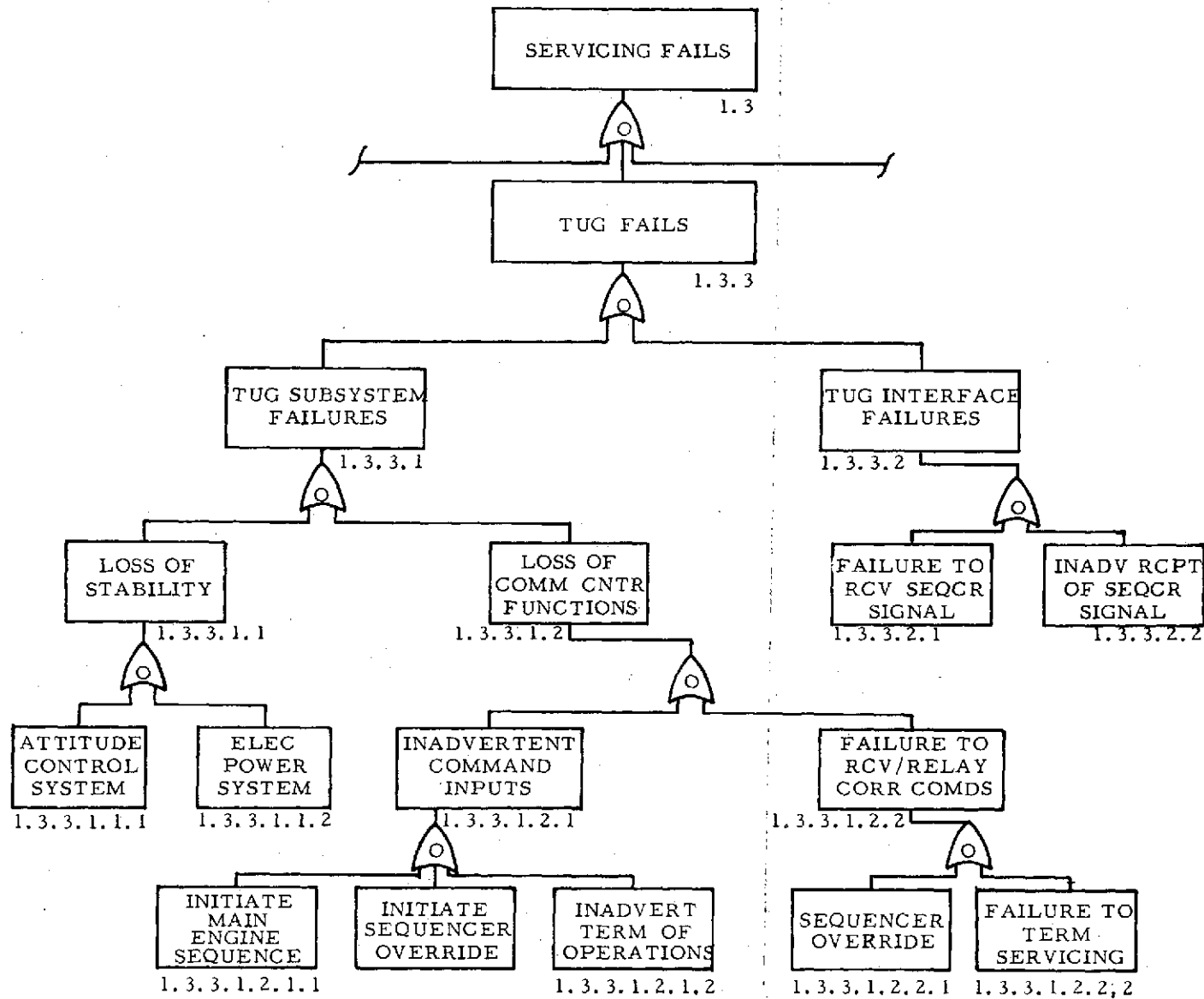


Figure 4-10. Tug Failures Which Preclude Servicing

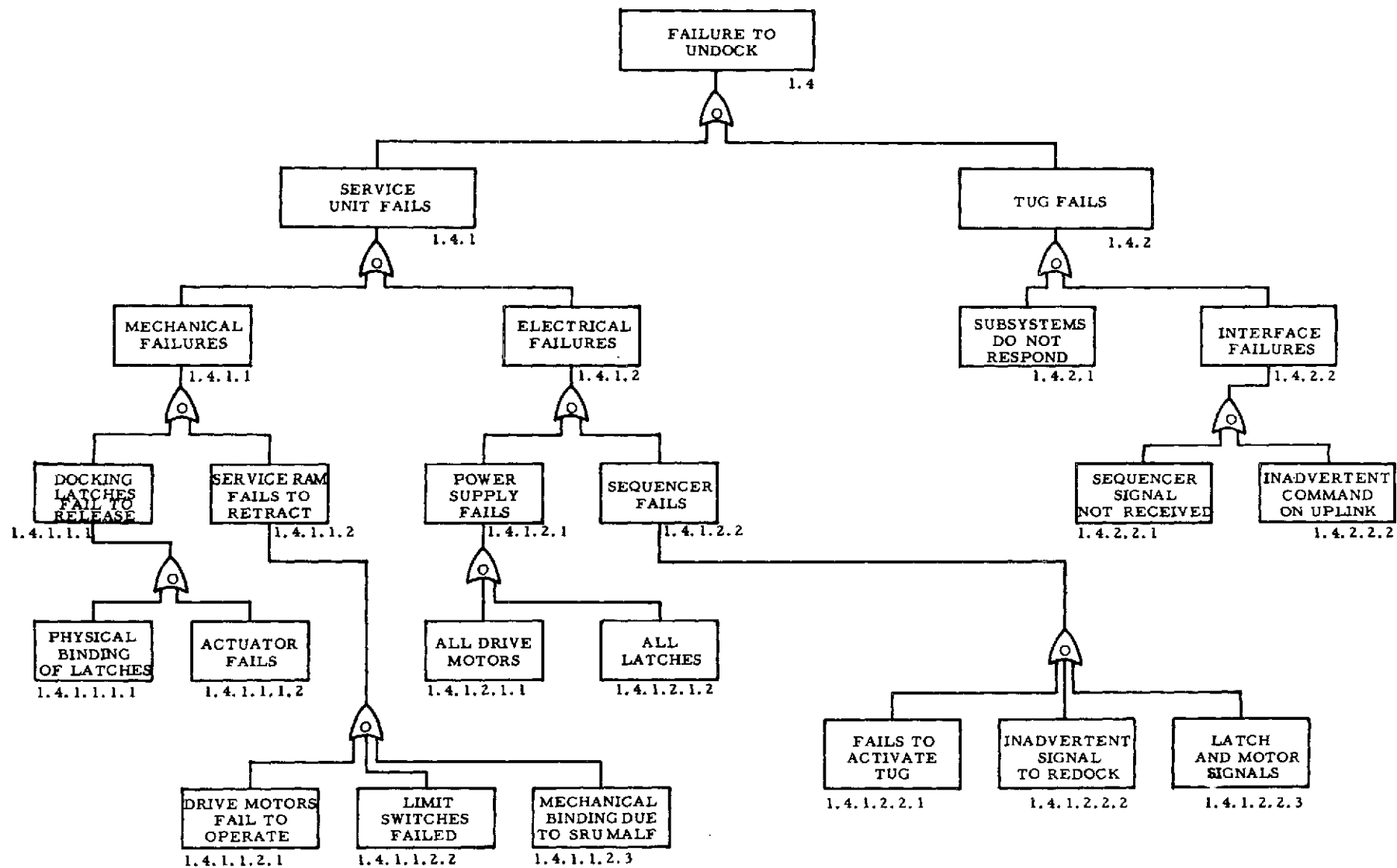


Figure 4-11. Failures Precluding Payload Separation



A similar command override capability is desirable for upper stage failures that could preclude the undocking action. Visual observation is desirable, but it is difficult to conceive of an approach that would afford the proper visibility. In any event, the uniqueness of the situations seem to dictate the need for active reasoning by the operations center, even if the input intelligence is limited to telemetry data.

This completes the development of the fault tree founded upon a top event of "Servicing Mission Fails." The sub-branches are reasonably complete for addressing the question of manned interactive support for space servicing. The trees could be expanded further and reliability data incorporated to derive redundancy requirements. The need for redundant elements is obvious from examination of the trees, in many instances even without statistical data. However, it is extremely difficult to estimate man's contribution to the reliability of the total system. Consequently, it was not attempted for this effort. Instead, experience and prudent judgment have been employed to arrive at what should be recognized as reasonable conclusions for the task at hand. The results and conclusions are presented in the next section. Further clarification of each block of the tree is provided in the hazard analysis, presented in the Appendix.

## 5. RESULTS AND CONCLUSIONS

Looking at the total problem of space servicing contingencies, it is now possible to draw certain conclusions. These must be considered in light of the fundamental assumptions presented in Section 2. Although a firm definition of the hardware and operational approach is not available, it is shown that a review of this type can aid in the process of developing program requirements. Therefore, the following conclusions are provided.

### 5.1 HARDWARE DESIGN

There were no significant hardware design problems exposed. This includes consideration of the upper stage, the service unit and the payload. Space servicing does not appear to push the state of the art and, in fact, the majority of operations can be automated in the same manner as existing operational programs of today.

### 5.2 REDUNDANCY LEVELS

The levels of redundancy for the upper stage and service unit need to be carefully reviewed. Current design approaches for the upper stage in general provide little redundancy due to the desire to minimize inert weight. However, the Shuttle upper stage will be required to perform missions wherein high cost payloads and operations are involved. This analysis indicates several areas where redundancy should be considered to support space servicing. The navigation computer or its elements, the command receiver and transmitter, and interface signals with the service unit should be redundant, to identify a few of the areas of concern.

The service unit should have redundancy in all mechanical/electrical components. The weight penalty should be small. The potential problems associated with drive systems for indexing and translating SRUs cannot be allowed to hang up the units midway in the process. Some means must always be available to back out of this type of situation. The rendezvous laser and video camera may not have to be redundant. Since they provide

alternate paths to accomplish the mission, it may be possible to get by with single units. However, thorough reliability analyses should be performed. Redundant power supplies and power distribution are a must. Failure of these elements could be catastrophic.

### 5.3 MANNED INTERACTIVE SUPPORT

In light of the several conditions exposed by the fault tree, it is recommended that active manned support be provided for the servicing operations. Basic upper stage and service unit operations should be automated to relieve the ground of any heavy support requirements. However, one man, supported by telemetry data, should have visual contact with the payload at all times during the docking maneuver. He should also have the command authority to override and alter automated sequences. This should not pose any serious technical problems and the recurring cost at the mission control center should be very minimal. The advantages of man-in-the-loop are limited and should be considered objectively. The required hardware will inherently increase the design complexity. It will also reduce the mass fraction. Also, it may not provide any real improvement for the payload. If the payload has failed in a manner that precludes servicing, then the best that can be hoped for is to not lose the upper stage while trying to perform servicing. Visual contact can help in this case. SRU replacement procedures can be readily automated and the contingencies that could evolve would probably not be enhanced by the visual monitoring system. An alternate fibre optics approach might prove otherwise and deserves further consideration. A command override capability is required to restart, reverse, or alter the sequencer. The sequencer could be a small computer with redundant logic and input/output channels. The hangup, if any, will probably occur not in the sequencer, but in the various drive mechanisms. For this reason, whatever design is selected, every effort should be made to minimize the number of motions required to replace SRUs.

#### 5.4 PAYLOAD FAILURE ISOLATION

Finally, it is important to emphasize that failure identification must be positive and absolute prior to initiating a service flight. This is the responsibility of the payload user. The failure need only be isolated to the SRU level, but it also must be known if more than one SRU should be replaced. Therefore, it may be possible to reduce the level of telemetry to be transmitted to and analyzed at the payload operations center. An in-depth study should be performed on this subject. Obviously, replacing the wrong SRU would be embarrassing and costly. However, there is also a history of instrumentation sensors providing false warnings resulting in unnecessary equipment changes. Therefore, a reduction in telemetry should be favorable if the proper information is available for positive isolation to the SRU level.

In summary, it should be stated that every effort was made to be objective with this analysis. There are obvious advantages of manned interactive support, but there are also obvious disadvantages. Space servicing is a complex operation, but on the other hand, the potential cost benefits indicate that this direction should continue to be pursued and developmental programs instigated.

## REFERENCES

1. Operations Analysis (Study 2.1), Shuttle Upper Stage Software Requirements, ATR-74(7341)-4, The Aerospace Corporation, El Segundo, California (15 July 1974).
2. Operations Analysis (Study 2.1) Payload Designs for Space Servicing, ATR-74(7341)-3, The Aerospace Corporation, El Segundo, California (30 June 1974).

## APPENDIX

### SPACE SERVICING HAZARD ANALYSIS

1.0 Geosynchronous Operations Only

BLOCK NO.	BLOCK TITLE	FUNCTIONAL DESCRIPTION	HAZARD DESCRIPTION	EQUIPMENT INTERFACES	HAZARD RANK*				
					1	2	3	4	5
1.0	Service Mission Fails	<p>A service mission includes four elements for consideration:</p> <ol style="list-style-type: none"> <li>1. The Tug vehicle</li> <li>2. The service unit (SU)</li> <li>3. The payload; and,</li> <li>4. The mission control center (MCC)</li> </ol> <p>Failure of any one or more of these elements can lead to a failure to perform servicing. Failure to perform servicing results in a cost increase either because the service capability is forfeited or as a minimum it must be repeated.</p> <p>(For the purpose of this study, the NASA Full Capability Tug has been assumed to be the Shuttle upper stage.)</p>	<p>Any action, or lack of action, which prevents a successful service mission is considered to be a hazard. These have been grouped into the following conditions:</p> <ol style="list-style-type: none"> <li>1. Catastrophic collision</li> <li>2. Failure to rendezvous &amp; dock</li> <li>3. Failure of servicing; and,</li> <li>4. Service complete but failure to undock.</li> </ol>	<p>Tug Service Unit Payload MCC MSFN</p>	N/A	N/A	N/A	N/A	N/A

# 1.1 Catastrophic Collision Occurs

BLOCK NO.	BLOCK TITLE	FUNCTIONAL DESCRIPTION	HAZARD DESCRIPTION	EQUIPMENT INTERFACES	HAZARD RANK*				
					1	2	3	4	5
1.1	Catastrophic Collision Occurs	Any action resulting in physical contact between the various elements other than the planned docking mechanisms is considered to be a catastrophic collision. The three elements involved are.  1. Tug 2. Service Unit 3. Payload	1. Inadvertent physical contact may puncture a Tug propellant tank or sensitive equipment package preventing the Tug from continuing the mission.  2. Inadvertent physical contact of the service unit could displace the SU relative to the Tug, preventing subsequent rendezvous with the Shuttle.  3. Inadvertent physical contact with the payload could result in permanent damage to NRU's or cause obstructions which prevent SRU replacement, terminating the use of the payload.	Tug Service Unit Payload MCC Command and Control Payload User Command and Control		X			X
1.1.1	Tug Fails	Tug does not perform correctly within defined constraints and inadvertently impacts on payload	Tug systems fail to respond to commands, thereby losing control of the vehicle	ACS Power Rendezvous Sensors Comm			X		
1.1.1.1	Tug Subsystems Fail	Failure of Tug subsystems can result in a catastrophic collision if, and only if, the Tug is on a collision course.	Subsystem failures involved with terminal phase rendezvous including possible inadvertent command inputs.	ACS Power Rendezvous Sensors Comm	X		X		
1.1.1.1.1	Collision course	Normal operation requires Tug insertion to occur below and behind the payload. Improper insertion could place the Tug on a collision course.	Main propulsion has long burn. Navigation sensor errors. Thrust attitude bias Computer errors or improper updates.	ACS Main Propulsion System G&C Comm System		X			
1.1.1.1.2	Attitude Stabilization Fails	Three axis stabilization is required for this terminal phase rendezvous, including attitude hold during thrusting.	Proper alignment at impact cannot be maintained. Proper closure delta V cannot be maintained.	G&C Power fails Comm System (Ref plattitude) RCS fails - off or on			X		

(1) UNLIKELY TO OCCUR  
(2) WORK AROUND APPARENT  
(3) SIMPLE REDUNDANCY

(4) COMPLEX REDUNDANCY REQ.  
(5) MANNED INTERACTION REQ.



1.1 Catastrophic Collision Occurs

BLOCK NO.	BLOCK TITLE	FUNCTIONAL DESCRIPTION	HAZARD DESCRIPTION	EQUIPMENT INTERFACES	HAZARD RANK*				
					1	2	3	4	5
1.1.1. 1.2.1	Attitude Bias Errors	Proper attitude hold is required for laser radar search for PL acquisition and final docking action.	Laser fails to lock on PL and Tug is on collision course, or improper attitude at docking results in premature impact.	Attitude control system Comm system		X	X		
1.1.1. 1.2.2	PL Reference Attitude Error	The payload is commanded to a reference attitude for docking prior to power down. This reference must be input to the Tug for proper positioning.	Failure to achieve proper positioning may result in impact with structure other than the docking mechanisms	Comm system Payload ref			X		
1.1.1. 1.2.3	Nonresponse	Attitude control system must respond to error inputs to maintain stability	Loss of stability of Tug with resultant loss of laser lock and possible impact.	Attitude control system			X		
1.1.1. 1.2.4	Tumbles Tug	Failure could result in tumbling motion of Tug.	If tumbling occurs after final closure is initiated, collision could result.	Attitude control system			X		
1.1.1. 1.3	Navigation System Errors	Navigation system must maintain proper terminal phase velocity vector, including standoff maneuver.	Errors of the Nav system can result in high velocity impact or failure to perform standoff.  Hazard exists if, and only if, backup ground command does not function properly.	Nav sensors Nav computer Power fails SU Interface MCC comm link.		X			
1.1.1. 1.4	Communication System Fails	Comm system provides backup to Nav system by TM of ranging signals as well as use of TV when in range.	Fail to receive commands negates backup capability.  Inadvertent action could override Nav system commands.	SU signals Command receiver/ decoder MCC input commands Power			X		
1.1.1. 1.5	Propulsion Fails to Stop Tug	The ACS is used for Tug translation control and is required to establish the proper closure velocity ( $\approx 1$ fps)	Failure could result in low velocity impact with bounce and rotation of PL. High velocity impact could damage docking system or PL.	ACS Power Nav system			X		

(1) UNLIKELY TO OCCUR  
(2) WORK AROUND APPARENT  
(3) SIMPLE REDUNDANCY

(4) COMPLEX REDUNDANCY REQ.  
(5) MANNED INTERACTION REQ.

1.1 Catastrophic Collision Occurs

BLOCK NO.	BLOCK TITLE	FUNCTIONAL DESCRIPTION	HAZARD DESCRIPTION	EQUIPMENT INTERFACES	HAZARD RANK*				
					1	2	3	4	5
1.1.1. 1.5.1 & 1.1.1. 1.5.2	Fails On  Fails Off	ACS propulsion is required for positive control of relative motions between Tug and payload	Fail on condition can force high impact velocities. Fail off can fail to break relative velocities.	ACS Power G&C signal interface			X		
1.1.1. 2	Tug/Service Unit Interface Signals Fail	Rendezvous and docking data as well as sequencer signals must be relayed across the service unit/Tug interface.	Tug interface connections fail to pick up or inadvertently pick up sensor signals from SU	Service unit Interface connectors			X		
1.1.1. 2.1	Laser Ranging Signals Erroneous	Laser ranging signals are required by Tug navigation system to perform terminal phase maneuver	Intermittent or complete loss of signals can result in loss of Tug velocity control and standoff maneuver	Service unit Interface connectors		X	X		
1.1.1. 2.1.1 & 1.1.1. 2.1.2	Power System Fails or Sensor Fails	Failure of these items results in loss of laser data on the Tug side of the interface	Loss of Tug velocity control	Service unit Interface connectors and sensors		X	X		
1.1.1. 2.2	PL/SU Interface Switch Fails	The docking switch is required to shut down Tug rendezvous action once a latch up has been achieved.	Failure to receive signal can result in continued thrust by Tug, imposing high g loads on payload with resultant collapse of appendages.	Docking probe/drouge switch SU power SU sequencer	X	X			
1.1.1. 2.3	TV System Fails	Visual Inspection by use of TV is required during standoff to assure removal of all obstructions.	Failure of TV can lead to Tug impact of PL structure if payload commands fail to retract appendages.	TV sensor MCC comm link Power		X			X
1.1.1. 2.3.1  1.1.1. 2.3.2 & 1.1.1. 2.3.3	Power, Lights or Sensor Interface Signals Fail	These items are required for use of the TV by MCC. If natural lighting conditions warrant, aux lights can be removed	Improper action could lead to impact of PL structures	TV sensor MCC comm link Power		X	X		X

(1) UNLIKELY TO OCCUR  
(2) WORK AROUND APPARENT  
(3) SIMPLE REDUNDANCY

(4) COMPLEX REDUNDANCY REQ.  
(5) MANNED INTERACTION REQ.

# 1.1 Catastrophic Collision Occurs

BLOCK NO.	BLOCK TITLE	FUNCTIONAL DESCRIPTION	HAZARD DESCRIPTION	EQUIPMENT INTERFACES	HAZARD RANK*				
					1	2	3	4	5
1.1.2	Payload Fails	The payload must perform certain functions in order that servicing can be performed. Isolation of the failed module is assumed to occur prior to the need for servicing. This failure could manifest itself in disallowing the required functions to be performed	Payload will not be in proper configuration to support docking which could lead to a loss of the payload, a loss of the Tug, or a loss of the service unit	Payload subsystems User command control link			X		
1.1.2.1	Fails to Power Down	The payload is to power down prior to docking to prevent a reaction to the docking/servicing action.	Attitude control will be active at the time of docking. Inadvertent commands may be transmitted by command/receiver, and power must be removed from SRU to prevent arcing during change-out/replacement	Payload command link	X		X		
1.1.2.1 & 1.1.2.2	Disturbance Occurs and PL Fails to Respond	The payload must hold a constant attitude relative to the Tug within $\pm 5^\circ$ to assure proper probe and drogue contact.	If a disturbance occurs after power down, the relative attitude error can exceed limits leading to structural impact.	Power system Comm system			X		
1.1.2.2	Structural Failure of PL	Payload structural failures due to mechanical or pressure vessel failures may result in unpredictable obstructions in the docking path	Structural interference between Tug/SU and PL leading to structural damage of all three or entanglement leading to loss of all three vehicles.	PL appendages Comm system Power system					X
1.1.2.2.1 & 1.1.2.2.2	Unwanted Obstructions in Docking Path	Obstructions may result from failure of appendages to retract or a shift in an SRU position due to the explosive nature of adjacent pressure vessels.	Obstruction of docking mechanisms or failure to allow latch up due to SRU displacement	PL pressure vessels PL appendages					X
1.1.2.2	Distorted PL Frame	The payload frame must maintain the correct configuration to allow docking to occur.	Structural failures can result in an unsatisfactory configuration to support servicing	PL physical interfaces	X				

(1) UNLIKELY TO OCCUR  
(2) WORK AROUND APPARENT  
(3) SIMPLE REDUNDANCY

(4) COMPLEX REDUNDANCY REQ.  
(5) MANNED INTERACTION REQ.

# 1.1 Catastrphic Collision Occurs

BLOCK NO.	BLOCK TITLE	FUNCTIONAL DESCRIPTION	HAZARD DESCRIPTION	EQUIPMENT INTERFACES	HAZARD RANK*				
					1	2	3	4	5
1.1.2. 2.2.1 1.1.2. 2.2.2 1.1.2. 2.2.3	Launch, Thermal or Explosive Environment	The PL is designed to withstand specific environments for deployment and subsequent operation	These hazards, if not properly recognized, could result in a distorted spacecraft, requiring, but not allowing, servicing.	PL physical interfaces Pressure vessels Thermal paths	X				X
1.1.2.3	Fails to Retract Appendages	All appendages such as solar panels, antennas, sun shades must be out of the line-of-approach of the Tug. If such items are not normally clear, a command must be issued to clear the PL configuration for docking.	Appendages may cause structural impact. Positive identification of retracted position may be lost due to position switch failure.	Comm system Power SRU interfaces					X
1.1.2. 3.1 1.1.2. 3.2 1.1.2. 3.3 or 1.1.2. 3.4	Appendage Obstructs Dock Side and Structural Mechanical or Electrical Failures	All appendages must be retracted clear of line-of-approach. (Structural failure of payload itself is covered in 1.1.2.2)	The hazard occurs if, and only if, obstruction exists and the retraction mechanism fails to function correctly	Power Comm system SRU interface					X
1.1.2. 4	Fails to Orient	The payload is required to orient itself to admit the service unit docking mechanism.	Improper orientation, if unknown, will lead to structural impact of the SU and the PL.	ACS Power Comm link			X		
1.1.2. 4.1 and 1.1.2. 4.2	Failure to Receive Command and Failure of ACS	The command to reorient the PL attitude for docking will be given by the user ground station after the Tug insertion maneuver.	Improper orientation leading to structural impact.	Power ACS S&C			X		
1.1.2.4. 2.1 1.1.2.4. 2.2 1.1.2.4. 2.3	Power ACS and S&C system	These subsystems are required to perform the reorientation maneuver. Command is issued by user through coordination with MCC	Improper orientation leading to structural impact.	Comm system			X		

(1) UNLIKELY TO OCCUR  
(2) WORK AROUND APPARENT  
(3) SIMPLE REDUNDANCY

(4) COMPLEX REDUNDANCY REQ.  
(5) MANNED INTERACTION REQ.

# 1.1 Catastrophic Collision Occurs

BLOCK NO.	BLOCK TITLE	FUNCTIONAL DESCRIPTION	HAZARD DESCRIPTION	EQUIPMENT INTERFACES	HAZARD RANK*				
					1	2	3	4	5
1.1.3	Service Unit Fails	The service unit consists of indexing and drive motors for remove/replace SRU's as well as the rendezvous sensors and docking mechanisms.	Structural, mechanical or electrical failures of the service unit can result in unwanted structural impact with the payload	Tug interfaces Power system Sequence Payload interfaces			X		
1.1.3.1	Structural Failure of Service Unit	The service unit must be capable of servicing launch and orbit transfer without serious distortion	The docking surface is not planar to mate with the payload	Structural interfaces SRU to base-plate interfaces	X				
1.1.3.1.1 or 1.1.3.1.1	Distorted Frame or SRU displacement from Mount	The frame and SRU positions must remain within tight tolerance to prevent interface problems with the payload	Distorted from, or SRU impinges prematurely on payload with resultant structural interference which could negate undocking	SRU and structural interfaces	X				
1.1.3.2	Docking Sensors Fail	The docking sensors provide the data to the Tug navigation and control system and the comm system for relay to MCC.	Lack of signal or inadvertent error signals may result in the service unit (with Tug) impacting the PL at excessive velocity.	Tug/SU Interfaces Power Laser TV		X	X		
1.1.3.2.1 and 1.1.3.2.2	Laser Radar and TV Camera (with lights)	The laser radar is the primary source of data for rendezvous, with a TV system as backup when approaching the PL	Loss of laser data will result in impact if and only if, the TV system is also inoperative.	Power Tug/SU Interface Laser TV		X			X
1.1.3.2.3	Service Unit Power Supply	The power supply and power regulation supply the input power to operate the rendezvous sensors.	Failure of power makes all SU sensors inoperative and terminates steering signals across the interface which could cause impact	Power SU Sensors Sequencer			X		
1.1.3.3	Tug Electrical Interface Fails	Electrical connectors are required at the service unit interface with the Tug.	Failure of these interfaces results in loss of sensor data to the Tug Nav and control which could cause impact.	Power SU Sensors Sequencer			X		
1.1.3.3.1 and 1.1.3.3.2	Laser Loop Open and TV Signal Loop Open	The laser and TV are required for terminal rendezvous providing steering information to the Tug.	The hazard exists, if and only if, both sets of sensor data are lost and a relative delta V exists between the Tug and PL.	Laser TV Lights Power		X			X

(1) UNLIKELY TO OCCUR  
(2) WORK AROUND APPARENT  
(3) SIMPLE REDUNDANCY

(4) COMPLEX REDUNDANCY REQ.  
(5) MANNED INTERACTION REQ.

1.1 Catastrophic Collision Occurs

BLOCK NO.	BLOCK TITLE	FUNCTIONAL DESCRIPTION	HAZARD DESCRIPTION	EQUIPMENT INTERFACES	HAZARD RANK*				
					1	2	3	4	5
1.1.3.4	Oversize SRU Fails to Position	Oversize SRU's may be carried on the service unit requiring part of the SRU (antenna) to be folded in front of the SU. This SRU will be commanded to a clear position prior to docking.	Failure of SRU to reposition could result in structural damage of entanglement	SRU interface with SU Sequencer Power supply	X		X		
1.1.3.4.1 1.1.3.4.2 or 1.1.3.4.3	Sequencer Power or Mechanical Failures	This item must function as planned to remove SRU obstruction prior to docking.	Failure to respond or over positioning can lead to a structural impact or entanglement	Sequencer Power Physical			X		

(1) UNLIKELY TO OCCUR  
 (2) WORK AROUND APPARENT  
 (3) SIMPLE REDUNDANCY

(4) COMPLEX REDUNDANCY REQ.  
 (5) MANNED INTERACTION REQ.

# 1.2 Failure to Rendezvous and Dock

BLOCK NO.	BLOCK TITLE	FUNCTIONAL DESCRIPTION	HAZARD DESCRIPTION	EQUIPMENT INTERFACES	HAZARD RANK				
					1	2	3	4	5
1.2	Failure to Rendezvous and Dock	To perform a service mission it is necessary for the Tug/SU to hard-dock with the payload to exchange SRUs.	Failure to rendezvous and dock leads to a failure of the servicing mission. Failure may be caused by the Tug, service unit, or the payload.	Tug Service Unit Payload MCC	X				
1.2.1	Tug fails to rendezvous	To perform rendezvous it is necessary for the Tug to insert near the payload, acquire the payload to measure relative motion, and perform the terminal phase maneuver.	Failure of the Tug to perform any of these functions will result in failure to perform servicing.	Tug SU Payload MCC			X		
1.2.1.1	Tug fails to get into range	The insertion maneuver is to place the Tug below and behind the payload.	Failure to insert properly may result in the laser system not acquiring the payload.	Tug Main Propulsion System NAV System		X			
1.2.1.1 - 1.1 or 1.2.1.1 - 1.2 or 1.2.1.1 - 1.3	Navigation system fails or Main propulsion fails or Tug subsystems fail	All systems must function properly for the Tug to perform the insertion maneuver.	Failure of subsystems or the main propulsion will result in improper insertion maneuver with resultant loss of the servicing mission.	Tug Main Propulsion NAV System All Subsystems	X		X		
1.2.1.2	Tug in range but fails to respond	After insertion the Tug must continue to respond to steering commands acting through the ACS system. This system provides control of all degrees of freedom.	If, after inserting within range of the payload the Tug fails to respond to further commands, the mission is lost.	SU Interfaces Tug Systems Tug ACS System			X		
1.2.1.2.1	Navigation system failures	The navigation system develops all commands in a closed loop manner to control the Tug to rendezvous and dock.	Failure of the NAV system outside of visual (TV) range disallows performing the terminal phase rendezvous	Tug Service Unit Sensors Tug/SU Interface			X		
1.2.1.2.1.1	Fails to lock on to payload (140 sec scan)	The laser radar must lock onto the payload to obtain ranging information.	Failure to acquire the payload disallows the TPI maneuver	Laser Power Interface		X			

(1) UNLIKELY TO OCCUR  
(2) WORK AROUND APPARENT  
(3) SIMPLE REDUNDANCY

(4) COMPLEX REDUNDANCY REQ.  
(5) MANNED INTERACTION REQ.

# 1.2 Failure to Rendezvous and Dock

BLOCK NO.	BLOCK TITLE	FUNCTIONAL DESCRIPTION	HAZARD DESCRIPTION	EQUIPMENT INTERFACES	HAZARD RANK				
					1	2	3	4	5
1.2.1-2.1-1.1 and 1.2.1-2.1-1.2 or 1.2.1-2.1-1.3 or 1.2.1-2.1-1.4	Laser and TV fail or SU power or interconnects fail	The laser and TV require power from the service unit to function and the signals to the Tug are passed through interface data lines.	Failure of either sensor or the power supply or data leads will result in loss of mission.	Laser TV Power Interconnects			X		
1.2.1-2.1.2	Locks on erroneously	The laser must lock on the payload corner reflectors to obtain proper ranging information.	If the laser locks on some part of the payload other than the corner reflectors an improper return will be received indicating a different range. The Tug will not be able to close on the payload.	Laser Payload Corner Reflectors		X			
1.2.2	Service unit fails to dock	Docking mechanisms are contained within the service unit, consisting of a probe and locking latches.	Failure of the docking mechanisms prevents SRU changeout and causes the mission to fail.	SU Probe PL Drogue Docking Latches Inhibit Switches		X	X		
1.2.2.1	Mechanical failures	Mechanical latches are required for a positive and hard-dock, matching all interfaces accurately.	Mechanical failures may not allow a hard-dock, causing interference with the indexing and positional mechanisms.	Power Physical			X		
1.2.2-1.1	Probe fails to lock	The probe inserts and locks inside the drogue and then snubs up the payload to the service unit.	Failure of the locking latches prevents the snubbing actions, negating servicing.	SU Probe Drogue Power		X	X		

(1) UNLIKELY TO OCCUR  
(2) WORK AROUND APPARENT  
(3) SIMPLE REDUNDANCY

(4) COMPLEX REDUNDANCY REQ.  
(5) MANNED INTERACTION REQ.



# 1.2 Failure to Rendezvous and Dock

BLOCK NO.	BLOCK TITLE	FUNCTIONAL DESCRIPTION	HAZARD DESCRIPTION	EQUIPMENT INTERFACES	HAZARD RANK				
					1	2	3	4	5
1.2.2-1.1.1 or 1.2.2-1.1.2 or 1.2.2-1.1.3	Damaged Probe or Damaged Drogue or Electrical Failure	Both probe and drogue must be aligned properly. The electrical drive for disengagement and snubbing must also be inhibited.	Failure of these items will prevent a hard dock, disallowing servicing.	Probe Drogue Power		X	X		
1.2.2.2	Electrical Failures	The SU Electrical System provides power to snub, latch, index, and change modules, all controlled by a sequencer.	Failure of the electrical system disallows SRU changeout.	SU Power SU Sequencer			X		
1.2.2-2.1 or 1.2.2-2.2	Sequencer Fails or Main Power Fails	The sequencer and main power supply are required to perform the service function.	SU cannot index and perform module changeout or unlatch with PL.	SU Power SU Sequencer			X		
1.2.3	Payload Fails to Respond	The payload must be placed in the proper configuration to allow rendezvous and docking.	Failure to do negates rendezvous docking due to structural interference and attitude differences.	PL ACS System PL Comm System PL Power System			X		X
1.2.3.1 or 1.2.3-1.1 or 1.2.3-1.2	Fails to Retract Append. Mechanical or Electrical	Appendages that will obstruct the docking line of approach must be retracted.	Failure to do so will result in physical impact or cancellation of docking maneuver at stand off.	PL Power Physical Interfaces			X		X
1.2.3.2	Fails to alter attitude	The payload must assume the proper attitude for docking and once achieved this information should be relayed to the Tug to proceed.	Failure to reorient can result in failure of laser lock-on or improper lock-on and subsequent impact.	PL ACS PL comm. System PL Power PL G&C			X		

(1) UNLIKELY TO OCCUR

(2) WORK AROUND APPARENT

(3) SIMPLE REDUNDANCY

(4) COMPLEX REDUNDANCY REQ.

(5) MANNED INTERACTION REQ.

# 1.2 Failure to Rendezvous and Dock

BLOCK NO.	BLOCK TITLE	FUNCTIONAL DESCRIPTION	HAZARD DESCRIPTION	EQUIPMENT INTERFACES	HAZARD RANK				
					1	2	3	4	5
1.2.3-2.1 or 1.2.3-2.2 or 1.2.3-2.3 or 1.2.3-2.4	ACS Fails or Attitude Ref. Lost or Comm. System Fails or Power is Off	The subsystems must function as planned to assure that payload assumes the proper docking position.	Failure of any one of these will result in failure to reorient for docking.	PL ACS PL Comm. PL Power PL G&C			X		
1.2.3.3 or 1.2.3-3.1 or 1.2.3-3.2	PL orients to wrong attitude due to Attitude Ref. failure or Comm. System Failure	The payload must not only be able to alter attitude; it must also assume the correct attitude.	Failure to orient properly may result in failure to allow rendezvous and dock. Failure may occur due to bias error or comm. input error..	PL G&C PL Comm.			X		X
1.2.3.4	Fails to Power Down	Payload must be powered down after reorientation to prevent extraneous inputs which might alter the PL configuration.	Failure to do so could cause appendages to be extended, attitude to drift, etc., negating docking.	PL Comm. System Interface Switch			X		
1.2.3-4.1 and 1.2.3-4.2	Comm. System and Drogue Switch Failures	The communication system is the primary source of power-down command backed up by a drogue switch, energized by the SU probe.	Failure of both sources is required to prevent power-down. Appendage problems could still exist but power would be off during SRU changeout. The stand-off maneuver will identify if appendages have been retracted.	PL Comm. Interface Switch			X		

(1) UNLIKELY TO OCCUR  
(2) WORK AROUND APPARENT  
(3) SIMPLE REDUNDANCY

(4) COMPLEX REDUNDANCY REQ.  
(5) MANNED INTERACTION REQ.

### 1.3 Servicing Fails

BLOCK NO.	BLOCK TITLE	FUNCTIONAL DESCRIPTION	HAZARD DESCRIPTION	EQUIPMENT INTERFACES	HAZARD RANK				
					1	2	3	4	5
1.3	Servicing Fails	Servicing relies primarily on the service unit for all sequencing and changeout operations. The Tug provides stability and the payload is dormant.	Failure of any of the three elements may lead to a failure of the servicing function.	Tug Service Unit Payload			X		
1.3.1	Service Unit Fails	The service unit performs all latching, indexing and SRU changeout.	Failure of any subsystems drive motors or structural elements may result in failure of service unit.	Power Drive Motors Sequencer Latching Switches			X		
1.3.1.1	Mechanical Failures	Major functions of the service unit are mechanical consisting of a gear driven ring frame and linear jack screw SRU change mechanism.	Failure of the ring frame or jack screws may impart damage to the SU, SRU, or the payload.	Power Drive Motors Sequencer		X			
1.3.1-1.1 1.3.1-1.1.1 1.3.1-1.1.2 1.3.1-1.1.3 1.3.1-1.1.4	Circular Drive Motors Fail	Circular drive motors are engaged by the sequencer and energized to rotate the index ring clockwise or counterclockwise.	Drive motors may fail due to bearing heat up under heavy cycling or misalignment, or limit switches fail closed, terminating action or fail open, extending the rotation. Drive motors may also fail due to overheating of their field, etc. Each of these actions could result in failure to service payload.	Power Sequencer Limit Switches Drive Motors (same action relates to jack screw motors)			X		
1.3.1-1.2	Ram Drive Motors Fail	These motors are engaged by the sequencer and energized to actuate the SRU changeout ram. Limit switches are used to indicate extremes of position.	Failure of these motors may prevent servicing or leave the ram in an extended position which may be hazardous to both the service unit and the payload.	Power Drive Motors Limit Switches Sequencer			X		

(1) UNLIKELY TO OCCUR  
(2) WORK AROUND APPARENT  
(3) SIMPLE REDUNDANCY

(4) COMPLEX REDUNDANCY REQ.  
(5) MANNED INTERACTION REQ.

### 1.3 Servicing Fails

BLOCK NO.	BLOCK TITLE	FUNCTIONAL DESCRIPTION	HAZARD DESCRIPTION	EQUIPMENT INTERFACES	HAZARD RANK				
					1	2	3	4	5
1.3.1-1.2.1 1.3.1-1.2.2 1.3.1-1.2.3 1.3.1-1.2.4	Motor or Limit Switches Fail	Major functions of the service unit are mechanical consisting of a gear driven ring frame and linear jack screw SRU change mechanism	Failure of the ring frame or jack screws may impart damage to the SU, SRU, or the payload.	Power Drive Motors Sequencer			X		
1.3.1-1.3	Ring Frame Jams	The ring frame has a large bull gear inner surface in which drive motors are engaged by a sequencer signal. The ring frame will be locked in position during ascent phase of flights.	Hazards may result which jam the ring frame, preventing the servicing operation.	Power Sequencer Drive Motors		X			
1.3.1-1.3.1 1.3.1-1.3-1.1 1.3.1-1.3-1.2 1.3.1-1.3.2 1.3.1-1.3-2.1	Launch Locks Fail to Release or an Obstruction is in Gearway	Launch locks must be released before servicing can be performed, initiated by the sequencer.	Hazards may result if launch locks do not release, if there is mechanical damage, if the sequencer signal fails, or if an SRU fails and obstructs movement.	Power Sequencer Drive Motors Structural Failure			X		
1.3.1-1.4	Ram Mechanism Jams	The ram mechanism is engaged by the sequencer to remove and replace SRUs with limit switches at the extremities.	If the mechanism does not function properly the extended ram may damage the payload, service unit or SRUs.	Power Sequencer Drive Motors Limit Switches			X		
1.3.1-1.4.1 1.3.1-1.4.2	Inadvertent Actuation or Misalignment of SRU	Engagement and energizing is performed by the sequencer. Alignment is critical	Inadvertent actuation may bind up the service unit, damage an SRU or the payload. A misalignment (due to sequencer or limit switch failure) may also cause structural damage and interlock the payload and the service unit.	Power Sequencer Drive Motors Limit Switches			X		

(1) UNLIKELY TO OCCUR  
(2) WORK AROUND APPARENT  
(3) SIMPLE REDUNDANCY

(4) COMPLEX REDUNDANCY REQ.  
(5) MANNED INTERACTION REQ.

1.3 Servicing Fails

BLOCK NO.	BLOCK TITLE	FUNCTIONAL DESCRIPTION	HAZARD DESCRIPTION	EQUIPMENT INTERFACES	HAZARD RAKE				
					1	2	3	4	5
1.3.1.2	Electrical Failures	Service unit power is supplied by batteries to the sequencer, motors, and rendezvous sensors.	Failures may result in failure to actuate servicing or promote inadvertent actuation.	Power Sequencer Motors Limit Switches			X		
1.3.1-2.1 1.3.1-2.1.1 or 1.3.1-2.1.2	Main Power Fails, such as: Power Regulation or Battery Fails	Main power supplies all electrical energy to service unit failures.	Power failure may result in initiating an action but failing to complete it with resultant damage to the service unit, payload, or SRUs.	Power Sequencer Motors Limit Switches			X		
1.3.1-2.2 1.3.1-2.2.1 1.3.1-2.2.2	Power Distribution Fails, such as: Overload Protection Fails or Sequencer Inhibit Fails to Release	Power distribution is through a cable harness controlled by the sequencer energized upon physical docking with the payload.	If overload protection fails, a motor failure could result in a hangup of the servicing unit. Also if the sequencer fails to release inhibit functions for the drive motors the servicing cannot be performed.	Power Sequencer Motors Limit Switches			X		
1.3.1.3	Sequencer Failures	The sequencer controls all functions for servicing, being energized by the docking limit switch or a command signal through the Tug comm link.	Failure of the sequencer to issue signals when required or issuing erroneous signals may lead to disruption of the servicing function or cause physical damage or fail to release the payload after servicing.	Power Interface with Tug Limit Switch Controls			X		
1.3.1-3.1 1.3.1-3.2 1.3.1-3.3 1.3.1-3.4 1.3.1-3.4.1 1.3.1-3.4.2 1.3.1-3.4.3	Dock Probe Fails to Initiate or Sequencer Fails to Issue Signals or Sequencer Issues Erroneous Signal and Comm System Fails or Receiver Fails or Tug Power Fails or Interface Connector Fails	The sequencer can be overridden by ground command and through the Tug Command Receiver from MCC.	The hazards can exist, if and only if the backup command fails to be received at the sequencer. Sequencer failures could leave SRUs in a half in-half out condition. Failure of the command system could occur if the Tug receiver failed or if the Tug had a power failure or if the interface connection were broken.	SU Power Tug/SU Interface Tug Command Link Tug Power			X		X

(1) UNLIKELY TO OCCUR  
(2) WORK AROUND APPARENT  
(3) SIMPLE REDUNDANCY

(4) COMPLEX REDUNDANCY REQ.  
(5) MANNED INTERACTION REQ.

### 1.3 Servicing Fails

BLOCK NO.	BLOCK TITLE	FUNCTIONAL DESCRIPTION	HAZARD DESCRIPTION	EQUIPMENT INTERFACES	HAZARD RANK				
					1	2	3	4	5
1.3.2	Payload Fails to Respond	The payload must maintain a coplaner interface with the service unit to allow servicing to be performed.	Any obstruction which could prevent snubbing or module changeout.	Physical Interface SU to Payload		X			
1.3.2.1	Mechanical Interface Failure	The payload must maintain physical tolerances such that SRUs can be removed and replaced.	Structural damage could prevent module change, either by binding SRU or misalignment of ram mechanism.	Physical Interface SU to Payload		X			
1.3.2-1.1 1.3.2-1.1.1 1.3.2-1.1.2 1.3.2-1.1.1 1.3.2-1.1.2 1.3.2-1.1.1 1.3.2.1-1.1.2 1.3.2.1-1.1.3	SRU Interface Obstructions Caused by Failed SRU or Interference from Adjacent SRU Resulting from Electrical Connections or Binding of Guides or Fracture of a Component	Alignment of the SRU must be maintained for servicing. The free slot in the SU must align with the failed SRU and the replacement SRU must be lined up with the vacant payload slot.	Failure to maintain alignment may result in loss of servicing functions. Also misalignments may result in force fits causing SRU to bind up between the SU and PL resulting in permanent entanglement. If an SRU is fractured (failed structurally), the attempted removal may cause binding or damage to an adjacent SRU in which case servicing would be incomplete.	Physical Interfaces with NRU	X	X			
1.3.2-1.2	NRU Interface Obstructions	The NRU consists of the basic satellite framework and any other elements which are not replaceable, such as solar panels.	Any change in the physical interface of NRUs could prevent SRUs from being exchanged.	Physical Interface with SRU	X				
1.3.2-1.2.1 or 1.3.2-1.2.2	Cold Weld or Thermal Warpage	The SRU slides into the NRU on nylon roller, spring loaded guides and is snubbed to the frame by the action of making electrical contact.	Sliding surfaces may cold weld in space or be impaired due to thermal gradients. If this occurs, servicing cannot be completed and disengagement may not be possible.	Physical Interface between SRU and NRU	X				
1.3.2.2	Electrical Interface Failure	The payload is powered down prior to docking. No power crosses the interface. A backup power-down switch is provided in the docking probe in the event the command was not previously received.	No identifiable hazards present until after two failures. Hazard in the event two failures do occur is only minor.	SU Docking Probe PL Comm System			X		

(1) UNLIKELY TO OCCUR  
(2) WORK AROUND APPARENT  
(3) SIMPLE REDUNDANCY

(4) COMPLEX REDUNDANCY REQ.  
(5) MANNED INTERACTION REQ.

# 1.4 Failure to Undock

BLOCK NO.	BLOCK TITLE	FUNCTIONAL DESCRIPTION	HAZARD DESCRIPTION	EQUIPMENT INTERFACES	HAZARD RANK				
					1	2	3	4	5
1.4	Failure to Undock	The Tug and Service Unit must be capable of undocking with the payload to continue the mission.	Failure to undock may result in loss of the payload, Tug and service unit.	Tug Service Unit Payload		X			
1.4.1	Service Unit Fails	The service unit sequencer signals the Tug when servicing of a particular payload has been completed. This releases all latches and causes the Tug to perform a stand off maneuver.	Failure of the SU to perform its functions to disengage may lead to loss of all three elements.	Tug Service Unit Payload Sequencer Docking Latches			X		
1.4.1.1	Mechanical Failures	All docking and latching mechanisms as well as drive motors are grouped into this category.	Failure of latches or mechanical drives may prevent complete disengagement of the SU and payload.	SU Power SU Sequencer Latches Limit Switches		X	X		
1.4.1-1.1 1.4.1-1.1.1 or 1.4.1-1.1.2	Docking Latches Fail to Release Because Physical Binding Occurs or Actuators Fail	Docking latches are released by an electrical drive actuator signaled from the sequencer. The latch retracts to its stops, returning the signal to the sequencer.	Hazards can develop if any one of the latches fails to release. Failure of the electrical signal, or the actuator may occur, or if structural warpage is present a physical binding may result.	SU Power Sequencer Latches Limit Switches	X		X		
1.4.1-1.2 1.4.1-1.2.1 1.4.1-1.2.2 1.4.1-1.2.3	Service Ram Fails to Retract Because Drive Motors Fail to Operate or Limit Switches Fail or Mechanical Binding of SRU Occurs	The service ram (jack screw) extends past the interface with the payload. The drive motors are engaged by a signal from the sequencer. The ram retracts the failed SRU from the payload and inserts a new unit.	Failure of ram in an extended position will not allow indexing of the ring frame without damage to the PL and SU.	SU Power SU Sequencer Limit Switches Drive Motors			X		

(1) UNLIKELY TO OCCUR  
(2) WORK AROUND APPARENT  
(3) SIMPLE REDUNDANCY

(4) COMPLEX REDUNDANCY REQ.  
(5) MANNED INTERACTION REQ.

#### 1.4 Failure to Undock

BLOCK NO.	BLOCK TITLE	FUNCTIONAL DESCRIPTION	HAZARD DESCRIPTION	EQUIPMENT INTERFACES	HAZARD RANK				
					1	2	3	4	5
1.4.1.2	Electrical Failures	All latching, indexing, and replacements of SRUs requires electrical power.	Failure of electrical power will prevent the SU from releasing the payload, resulting in payload, SU and Tug loss	SU Power SU Sequencer Limit Switches Drive Motors			X		
1.4.1-2.1 1.4.1-2.1.1 1.4.1-2.1.2	Power Supply Fails. Results in Loss of All Drive Motors or All Latch Actuations	Electrical power is required intermittently to undock with the payload.	Power loss results in all drive motors and latches remaining in position when power failure occurs. Results in loss of PL, SU, and Tug.	SU Power SU Power Distribution			X		
1.4.1-2.2 1.4.1-2.2.1 1.4.1-2.2.2 1.4.1-2.2.3	Sequencer Fails Resulting in Loss of Tug Activation or Inadvertent Signal to Redock or Failure to Signal Latches and Motors	The sequencer performs a key function of managing all activities of the service unit except where override commands are issued by MCC.	Loss of power results in loss of sequencer operation which prevents undocking with the payload.	SU Sequencer SU Power			X		
1.4.2	Tug Fails	Upon receipt of the sequencer command, the Tug must separate from the payload and perform a stand-off inspection via the TV.	If the Tug fails to perform its function there will result a payload, Tug, and service unit loss.	SU Sequencer Comm System			X		
1.4.2.1	Tug Subsystems Do Not Respond	All Tug subsystems are required to function to perform the stand-off maneuver and continuation of the mission.	Failure of subsystems will result in loss of Tug, service unit, and payload.	All Tug Subsystems			X		
1.4.2.2 1.4.2-2.1 1.4.2-2.2	Interface Failures Resulting in Loss of Sequencer Signals or Inadvertent Command.	The service unit sequencer provides the signal to initiate Tug operations, backed up by a ground command from MCC. The signals then cross the interface from the SU to the Tug to activate Tug systems.	Loss of interface signals will prevent Tug activation, thereby resulting in loss of the Tug, SU, and payload.	SU/Tug Interface connections			X		

(1) UNLIKELY TO OCCUR  
(2) WORK AROUND APPARENT  
(3) SIMPLE REDUNDANCY

(4) COMPLEX REDUNDANCY REQ.  
(5) MANNED INTERACTION REQ.



THE AEROSPACE CORPORATION

EXTERNAL DISTRIBUTION LIST

(REFERENCE: COMPANY PRACTICE 7-21-1)

REPORT TITLE

Operations Analysis (Study 2, 1) Contingency Analysis

REPORT NO. ATR-74(7341)-5	PUBLICATION DATE 15 July 1974	SECURITY CLASSIFICATION Unclassified
MILITARY AND GOVERNMENT OFFICES	ASSOCIATE CONTRACTORS AND OTHERS	

(NOTE: SHOW FULL MAILING ADDRESS; INCLUDE ZIP CODE, MILITARY OFFICE SYMBOL, AND "ATTENTION" LINE.)

NASA Scientific & Technical  
Information Facility (3)  
P. O. Box 33  
College Park, Md. 20740

NASA - Headquarters  
Washington, D. C. 20546

V. N. Huff, Code MTE (50)

R. R. Carley, Code MTE (2)

Dr. J. W. Wild, Code MTE (1)  
New Technology Repr, Code KT (1)

NASA  
Mr. Duncan Collins  
P. O. Box 92960  
Worldway Postal Center  
Los Angeles, CA 90009  
Bldg. 120, Rm. 1406B (1)

AFR 80-45 DISTRIBUTION STATEMENT X'D BELOW APPLIES

☐ NO DISTRIBUTION STATEMENT  
(Classified documents only)

☐ A. APPROVED FOR PUBLIC RELEASE;  
DISTRIBUTION UNLIMITED

☐ B. DISTRIBUTION LIMITED TO U. S. GOV'T AGENCIES ONLY;

(Reason)

(Date statement applied) OTHER REQUESTS FOR THIS DOCUMENT

MUST BE REFERRED TO (Controlling DOD office)

APPROVED BY

*Robert R. Wolf*  
(FOR THE AEROSPACE CORPORATION)

DATE 7/9/74

APPROVED BY

(FOR COGNIZANT AF OFFICE)

(SYMBOL)

DATE

IF LIST COMPRISES TWO OR MORE SHEETS, COMPLETE  
THIS SIGNATURE BLOCK ON LAST SHEET ONLY

SHEET \_\_\_\_\_ OF \_\_\_\_\_